Telecommuting Guidelines for Managers

Telecommuting refers to the practice of fulfilling all or a portion of the employee’s work/job responsibilities at an alternative work site on a temporary basis while maintaining a full-time employment schedule. Telecommuting is not formally supported by the university and is not meant to be a permanent arrangement. Generally, a telecommuting arrangement is determined on a case by case basis. Should a temporary arrangement be needed it should not exceed a 4-6 week period. These guidelines inform the development, review, and approval of telecommuting requests to support the department or college’s business needs.

A telecommuting arrangement is most appropriate for a position that has clearly defined tasks, measurable work activity, and does not require the employee to be present in the office during all normal business hours. Based on business necessity, a manager may decide to ___ permit telecommuting at a department-wide or college-wide level.

Below are guidelines to assist managers in reviewing and approving a telecommuting request.

Before approving a telecommuting arrangement consider the following:

- Determine that the telecommuting arrangement supports the department, college and university’s goals, including cost effectiveness, excellent service, and high productivity.
- The impact of the telecommuting arrangement on the equitable work distribution, productivity, and communication needs among colleagues.
- Appropriate performance standards and measures will need to be in place.
- Established means of supervision, communication, and systems of accountability will need to be determined.

Procedure for Review and Approval

- Employee will submit a written request for a telecommuting arrangement that includes an explanation of the method that will be used to provide required services or work product.
- Review the request and determine if there is a business case for the requested arrangement. Is the arrangement feasible based on the type of work done, need for supervision, technology requirements, communication and work flow requirements, and required presence in the office?
- Determine, with the employee, the following:
  - Duration and schedule of the telecommuting arrangement
  - Methods and expectations of accessibility, communication, and accountability with management and co-workers while telecommuting
  - Technology requirements (telephone, voicemail, computer, internet access, etc.)
  - Maintaining the security of work related materials including documents saved on a computer and documents taken off-site. This also includes the safe destruction of confidential work-related documents. Refer to the university’s Information Security Policy and the attached Appendix A for additional information.
- Provide rationale for the approval or denial of the telecommuting arrangement.
- If approved, document the details of the telecommuting arrangement, including maximum length of time and equipment needs.
- Obtain the administrative or academic officer approval as appropriate.
• Maintain documentation on file within the department and have available to Human Resources upon request.
• Arrange any technology or equipment requirements.

Manager Responsibilities
• Be familiar with the Flexible Work Arrangement policy and Telecommuting Guidelines.
• Reiterate to the employee that the same standards of performance will continue to apply.
• Inform the employee that there may be mandatory on site meetings or other occasional on site events that will require the employee's attendance, regardless of the telecommuting arrangement.
• Establish a periodic review of the telecommuting arrangement.
• Review and track accurate time reporting (including work time, overtime, vacation time, and sick time).

A telecommuting arrangement can be discontinued by management with a three week notice, though an immediate and unanticipated operational need may require the immediate suspension of the telecommuting arrangement. The dissolution of a telecommuting arrangement by a manager should be based upon employee performance or the operational needs of the unit, and the rationale should be communicated to the employee in writing. An employee may request that the arrangement be discontinued. The granting or denial of such a request, and the timing of implementation if granted, is at management's discretion, based on business and operational needs.
Appendix A

The following technology related subjects should be addressed when determining a telecommuting arrangement.

**Equipment**

**Computer:**
The computer used during the telecommuting arrangement should be a DePaul owned laptop. The laptop should include “Computrace Data Protect – Advanced Theft/Data Protection”. The computer will have the DePaul image with the standard software. Computers will be monitored and maintained by DePaul’s centralized virus protection console and Windows update server. Use of the computer should be limited to the telecommuter for DePaul business. The computer should not be accessible via Windows remote desktop.

**DePaul support:**
Computers will be supported by DePaul IS via the Technology Contact Center (TCC).
Telecommuters may not use any external technical support service.
The TCC will provide phone support. Any issues that cannot be addressed via the phone will require the return of the computer to campus for additional support.

**Phone:**

**DePaul numbers**
It may be possible to have an IP phone at home with a DePaul University phone number. There are some technical requirements and restrictions. Information Services will assist in determining if this option is available for an individual. There is a cost associated with this option. If this is required, the department representative will need to speak with an IS representative via the Technology Contact Center.

**Technology:**

**Network:**
The telecommuter will require a high speed Internet connection. If utilizing a home wireless network, the wireless network must be secured appropriately with WPA encryption and non-default passwords.

**VPN:**
DePaul will provide a VPN that will allow the remote worker to access their DePaul email, Peoplesoft and network drives via a secure encrypted connection. Direct database access will not be available. Anyone that requires access to additional, specialized resources will need to contact an IS representative via the Technology Contact Center.

**Backup and DePaul Data:**
DePaul data must remain secure.
It is recommended that DePaul data be maintained on DePaul file servers (W and U drive). If it is necessary to keep this data locally, the data should be backed up on at least a weekly basis. If sensitive DePaul information is to be retained on paper, the telecommuter must have appropriate locking cabinets and a shredding device.

Policies:

The following University policies apply to DePaul University computers:
Acceptable Use Policy/Network Security
Access to and Responsible Use of Data