RUTGERS

School of Communication and Information
Rutgers, The State University of New Jersey
4 Huntington Street
New Brunswick, NJ 08901-1071

comminfo.rutgers.edu
Phone: 848-932-7500
Fax: 732-932-6916

Staff Telecommuting Policy
School of Communication and Information

Adopted January 1, 2020

The School of Communication and Information seeks to provide a workplace that supports the professional achievement and growth of all employees and the success of the school as a whole.   SC&I is adopting this Telecommuting Policy to make it possible for staff who wish to arrange for some telecommuting, and for whom it is appropriate to do so, to have that option within a framework that is supportive of them and fair and transparent to everyone.

Staff at SC&I fall into two workforce groups vis-a-vis university policies and contracts: (1) non-aligned employees classified as Managerial, Professional, Supervisory, and Confidential (referred to as "MPSC") and (2) those represented by the Union of Rutgers Administrators, URA-AFT, AFL-CIO Local 1766 (referred to as "URA-AFT").

Rutgers Policy 60.3.22 addresses issues of flexible workweeks and compressed workweeks for all employees, and telecommuting standards for MPSC staff. The ratified Rutgers / URA-AFT Local 1766 Agreement 2018-2022 addresses telecommuting standards for URA-AFT staff.

All provisions of these two policies are applied at SC&I; below is a summary of the provisions most relevant to SC&I:

- Staff who are exempt from the overtime provisions of the Federal Labor Standards Act may be eligible to be considered for telecommuting on a regular basis. Nonexempt employees – those who are paid overtime when they work more than forty hours in a week - are not eligible to be considered for telecommuting. This applies to both MPSC and URA-AFT staff.

- Not all exempt positions, and not all employees in exempt positions, will be suitable for telecommuting. Suitability is based on assessments of both the individual and the position the individual holds.

- Telecommuting is meant to be conducted from a single alternative work location and during the same work hours as the employee's normal work schedule. If an employee seeks to work different hours while telecommuting, that would essentially be two alternate work arrangements, flex-time and telecommuting. Both should be documented in the Telecommuting Agreement.

- The alternate work location should provide the employee adequate access to the tools necessary to do the job, including a chair and desk/table, lighting, telephone, computer, and internet connection. It is the employee's responsibility to provide all of these tools, unless a specific other arrangement is agreed upon with the school. Any such arrangements must conform to existing procurement and technology policies.

- The employee is responsible for assuring all university policies and procedures are followed at the alternate work location, including information technology security and use policies.

- Telecommuting does not change an employee's terms and conditions of employment.

- Telecommuting is not intended to give employees time to work at other jobs or attend to personal business.

- Telecommuting is not intended to circumvent other paid time off. For example, an employee who is too sick to come to work should take a sick day and not request a telecommuting day.

- Telecommuting is not intended, and cannot be used, as a substitute for dependent care. If one or more people in need of primary care are regularly present in the alternate work location when the employee is telecommuting, the employee must demonstrate that another individual is present to provide the care.

- Individuals who are telecommuting should be available to colleagues, faculty, and students via telephone and email just as they would be if they were present on campus.

- In the event of meetings on campus on an employee's regular telecommuting day, the supervisor may require the employee to come to the workplace but should give as much notice as possible.

- Any individual in a position that is suitable for telecommuting must have a positive performance review in order to be considered for telecommuting. If an employee has any performance ratings of "does not meet standards" or the equivalent, they will not be eligible for telecommuting. An employee who has a telecommuting arrangement in place whose work falls below standards will be asked to stop telecommuting.

- When a supervisor and employee discuss possible telecommuting:
  The employee must read and/or complete:
  (1) a Safety Self-Audit
  (2) the Information Technology Use Policy
  (3) the Request to Telecommute Form
  The supervisor must review all of the documents above and complete:
  (4) the Feasibility Assessment Telecommuting Policy Form
  And together the employee and supervisor must complete:
  (5) the University Telecommuting Agreement.
  (In addition, SC&I asks the employee to read the school's technology policy, as outlined in the next section.)

Once signed, all of these documents will be kept in the employee's personnel file.

There are many other details included in University Policy 60.3.22 and the URA-AFT contract which apply at SC&I. Anyone requesting to telecommute, and any supervisor involved in a discussion of telecommuting with an employee, should read all of the applicable documents.

TELECOMMUTING AT SC&I

The school will identify for any interested staff member whether they meet the three criteria to be able to request telecommuting:

(1) Whether their position is exempt or non-exempt from overtime provisions of FLSA, since the university has defined that only exempt positions may be eligible for telecommuting.
(2) For exempt employees, whether given the nature of the work they do, their position is considered by the school to be eligible to request regular telecommuting.
(3) If the employee is ineligible to telecommute because of ongoing performance issues.

Staff who meet the criteria and have been employed at SC&I for more than three months may request to telecommute. They need not give a reason why they want to telecommute. The supervisor will review the requirements for telecommuting with the employee. As part of that discussion the supervisor will ask if there are any potential distractions at the alternate work location during working hours, and if so, to outline what the plan is to address them.

Employees will be approved to telecommute a maximum of one day per week on a regular basis. Arrangements may be made to telecommute less often than once a week. When telecommuting is approved, the minimum amount of time for telecommuting on each regular day will be half a day.

In addition to the documents required by the university policies, SC&I employees who will be telecommuting are asked to review the SC&I Technology Policy in detail, especially the sections on use and security of information.

All employees should exercise judgment in requesting alternate work arrangements of any kind. Employees who are eligible to request to telecommute should consider their own work style and personal situations and whether telecommuting is a positive option for them. If a staff member who was telecommuting wishes to stop the arrangement for any reason, they may do so at any time.

As noted in the university policy, any staff member who is telecommuting whose productivity or quality of work falls below standards will be asked to stop telecommuting.

Because Wednesdays are typically used for departmental and other meetings at SC&I, staff will not be approved to telecommute regularly on Wednesdays.

In workgroups where more than one person is approved to telecommute, the supervisor will work out with staff which day each person will telecommute. If a consensus cannot be found, the supervisor has the authority to determine which employee will telecommute on which day.

If one or more employees within a work group call out sick, a supervisor may ask a telecommuting employee to come to the office. In such a case, the commute to work may take place during work hours since the employee would not likely be notified in time to arrive at their normal start of work. When this happens, a substitute telecommuting day may or may not be possible, depending on the needs of the workgroup, and the supervisor will make that determination.

All supervisors and employees at the school meet regularly to discuss plans for work and review of accomplishments; this is true for both telecommuting and non-telecommuting staff. However, in cases of telecommuting, each supervisor and telecommuting employee are asked to schedule a regular meeting once each week to hold such discussions.

On days of inclement weather when Rutgers-New Brunswick offices are open, individuals will not be permitted to telecommute in lieu of coming to campus unless it is their regular telecommuting day.

For security purposes, employees who are telecommuting must arrange to be able to VPN into their desktop so that it is possible for the documents or services they work on that require security to remain on the Rutgers network or secured on their office system or shared drive. Individuals who have Rutgers-issued laptops because of the needs of their positions may work on those laptops on telecommuting days.

Telecommuters are expected to take advantage of Rutgers' and SC&I's videoconferencing capabilities in order to be able to participate fully in meetings and other discussions taking place on their telecommuting days.

Employees who are telecommuting should arrange to have their work phone calls forwarded to a home or cell phone.

- On a standard Rutgers telephone, press Call Forward on the top right of the phone.
- When you see the menu on the readout, you can choose to forward all calls by using "1" as your option.
- You will see Call Forwarding is Off by default. Press the right arrow key to change to On.
- Then press the down arrow key to get to the number field, and enter the phone number you want to forward your calls to.
- Then press Done on the right side.
- You will see a red light next to Call Forward at the top right.
- Then press Done on the keypad again.
- For a video of this process, go to https://www.screencast.com/users/Bloustein/folders/VoIP/media/0ff924d6-f18d-489f-9a7d-39c611163c52.
- For assistance on how to set this up, contact the IT Helpdesk.
- Don't forget to stop Call Forwarding when you return to the office.

Employees who make work-related phone calls from a home or cell phone are welcome to block their phone number from being displayed.

- To block your cell phone number from being displayed, enter *67 and then enter the number you wish to call (including area code) and tap Call. On the receiver's phone, a word such as "Private" or "Anonymous" will appear instead of your mobile number.

An employee who had a telecommuting arrangement who wishes to stop telecommuting should put the request in writing, and the supervisor should acknowledge it in writing. When a supervisor informs an employee that due to performance issues they are no longer eligible to telecommute, that notification should be put in writing. In both cases, copies of those written communications should be added to the employee's personnel file.

In rare cases there are emergencies such that one or more SC&I buildings cannot be occupied during a work day. In such cases all employees who work in that building may be asked to telecommute. Likewise, in rare cases an individual employee may have an emergency such as a car breaking down and may request an emergency telecommuting day or partial day. This is only appropriate when the emergency will allow the employee to conduct work during their emergency. The school reserves the right to approve or disapprove such an emergency request for both exempt and non-exempt staff members.

APPENDICES

Appendix 1	Rutgers Policy 60.3.22 – Alternative Work Arrangements and Telecommuting for Regularly Appointed Staff
Appendix 2	Sections of the URA-AFT contract 2018-22 on telecommuting
Appendix 3	University Self Safety Audit
Appendix 4	Rutgers Pollicy 70.1.1 – Acceptable Use Policy for Information Technology Resources
Appendix 5	SC&I Technology Policies
Appendix 6	University Request to Telecommute
Appendix 7	Feasibility Assessment Telecommuting Policy Form
Appendix 8	University Telecommuting Agreement

RUTGERS POLICY

Section: 60.3.22

Section Title: HR/Non-Academic Employees

Policy Name: Alternative Work Arrangements and Telecommuting for Regularly Appointed Staff

Formerly Book: n/a

Approval Authority: Senior Vice President for Administration

Responsible Executive: Senior Vice President for Administration

Responsible Office: University Human Resources

Originally Issued: n/a

Revisions: 7/1/2013, 9/9/2013 (Updated title and Section 3)

Errors or changes? Contact: policies@hr.rutgers.edu

1. Policy Statement

Regularly appointed staff employees may be eligible to participate in alternative work arrangements in specific circumstances including telecommuting.

2. Reason for Policy

To provide guidelines on eligibility criteria for alternative work arrangements including telecommuting. Alternative work arrangements can facilitate accomplishing several objectives: achieving greater administrative efficiency; addressing current environmental concerns such as traffic congestion, air pollution, and transportation costs; improving employee productivity and performance; enhancing employees' work-life balance; supporting business continuity plans; and sustaining the hiring and retention of a highly qualified workforce.

3. Who Should Read This Policy

This policy is applicable only to employees in Rutgers positions. A Rutgers position is a position which, historically, was associated with the Rutgers University before June 30, 2013. Individuals employed in Rutgers positions are processed through the PeopleSoft (RIAS) payroll system. These positions may be governed by different negotiated agreements and policies from those that would be applicable to individuals in legacy UMDNJ positions. In this regard, individuals employed in Rutgers positions may be eligible for different non-State benefits than individuals who hold legacy UMDNJ positions.

4. Related Documents

Policy 60.3.14, Overtime for Regularly Appointed Staff
Policy 60.3.15, Additional Compensation for Full-Time Staff Members with "NL" Titles
Telecommuting website (http://uhr.rutgers.edu/worklife-balance/telecommuting)

- Guidelines on Telecommuting
- Telecommuting Agreement
- Telecommuting Proposal
- Telecommuting Feasibility Worksheet
- Safety Checklist

5. **Contacts**
University Human Resources
Office of Labor Relations: 848-932-3020

6. **The Policy**

60.3.22 ALTERNATIVE WORK ARRANGEMENTS FOR REGULARLY APPOINTED STAFF EMPLOYEES

I. Definitions

A. Alternate Work Location: a location other than the official university place of business from which an employee telecommutes.

B. Department Head: the person with the ultimate approval authority in the unit, or his or her designee.

C. Exempt: not subject to the overtime provisions of the Fair Labor Standards Act. (Employee titles coded as NL, NC, and N4)

D. Hours Worked: for fixed workweek staff; hours computed by adding all hours actually worked during the workweek plus any paid time off, such as vacation and sick time, except as modified by collective negotiations Agreements.

E. Non-exempt: this is a fixed workweek; employees are subject to the overtime provisions of the Fair Labor Standards Act. (Employee titles coded as 35, NE, and 40)

F. Telecommuting: a work arrangement in which an employee performs his or her regular job duties in an alternate location to the official university place of business.

G. Work Location: any on- or off-campus property that is owned, occupied, leased, or used by Rutgers University at which the employee is regularly assigned to attend work. This includes all research sites and all leased indoor and outdoor spaces or spaces occupied with a user permit, license, or contract for the conduct of university business.

II. Alternative Work Arrangements for Regularly Appointed Staff Employees

The definitions for all terms utilized in this Section (II) are the same as those utilized in Section I above unless otherwise noted.

A. Forms of Alternative Work Arrangements

The University recognizes two forms of alternative work arrangements: a flexible Work Day Arrangement and a Compressed Workweek Arrangement. Both forms of Alternative Work Arrangements may be implemented either department-wide or on an individual basis. The implementation of Alternative Work Arrangements shall be at the discretion of the employee’s work unit. Prior to implementing any form of alternative Work Arrangement for union-eligible staff, departments must contact the Office of Labor Relations.

1. Flexible Work Day Arrangement

The features of a flexible Work Day Arrangement are as follows:

a. A variable daily schedule that revolves around a fixed set of core hours, which may vary by employee;

b. A pre-defined start time during which the employee will commence his or her workday; for non-exempt[1] staff, a workday that remains for a specific number of hours (i.e. 7, 7.5 or 8), not including a meal break, during which the employee must be at work; and

c. A meal break of at least thirty (30) consecutive minutes.

2. Compressed Workweek Arrangement

a. Features of a Compressed Workweek Arrangement

The following features of a Compressed Workweek Arrangement are as follows:

i. A regularly repeating weekly, or bi-weekly, schedule that is shorter than five uniform and consecutive days in one workweek, or ten uniform and consecutive days in two workweeks, respectively;

ii. A regular workweek (e.g. 35, 37.5 or 40 hours) that is executed over the shortened period of time so that there are fewer but longer days in the new workweek(s);

iii. For non-exempt staff, a workday that is for a specific number of hours, not including a meal break, during which the employee must be at work;

iv. A meal break of at least thirty (30) consecutive minutes; and

v. One regularly scheduled day off that the employee receives as a result of the compression of the workweek(s). The regularly scheduled day off may be any day during such workweek(s), as predetermined by the department, which shall repeat with regularity.

b. The Two Forms of Compressed Workweek Arrangements

i. *4&1* In a 4&1 Compressed Workweek Arrangement the employee will work four (4) days and receive one (1) regularly scheduled day off in each workweek.

An employee who is in a 35-hour per week position and who is placed on a 4&1 compressed Workweek Arrangement will work four 8.75 days per workweek.

An employee who is in a 37.5-hour per week position and who is placed on a 4&1 Compressed Workweek Arrangement will work four 9.38-hour days per workweek.

An employee who is in a 40-hour per week position and who is placed on a 4&1 Compressed Workweek Arrangement will work four 10-hour days per workweek.

ii. *9&1* In a 9&1 Compressed Workweek Arrangement the employee will work nine (9) days and receive one (1) regularly scheduled day off in every two consecutive workweeks. A 9&1 Compressed Workweek Arrangement must correlate with an employee's pay period as defined in Section I above. A 9&1 compressed Workweek Arrangement is not available to overtime-eligible employees.

[1] The term non-exempt refers to those employees who are not exempt from the overtime provisions of the Federal Fair Labor Standards Act.

NL employees NL employees have a minimum average workweek of 37.5 hours. Accordingly, An NL employee who is placed on a 9&1 Compressed Workweek Arrangement will work nine days of at least 8.33 hours per two consecutive workweeks.

N4 employees N4 employees are required to work a minimum of 40 hours per workweek because their primary function is to directly supervise non-exempt, 40-hour, fixed workweek employees. Accordingly, an N4 employee who is placed on a 9&1 Compressed Workweek arrangement will work nine 8.9-hour days per two consecutive workweeks.

B. Alternative Work Arrangements for Part Time Employees

Compressed Workweek and flexible Work Day Arrangements can be implemented for part-time employees by following the same guidelines set forth in section A above, prorated according to the employee's part-time percentage.

C. Holidays and other Paid Leave Days

1. The value of a holiday or paid leave day is equal to 1/5 of the employee's regular workweek (e.g. 35, 37.5 or 40 hours, or less as in the case of part-time employees).

2. If a holiday falls or paid leave day is taken on an employee's regularly scheduled day of work, the employee shall receive the day off. If due to the compressed Workweek Arrangement the length of the employee's workday is greater than the value of the holiday or paid leave day, the difference must be charged to another form of time or to leave without pay.

3. If a holiday falls on an employee's regularly scheduled day off, the employee shall receive an alternate day off within the same workweek. If due to the Compressed Workweek Arrangement the length of the employee's workday is greater than the value of the holiday, the difference must be charged to another form of time or to leave without pay.

4. If an employee is directed to work on a holiday, the employee shall receive pay for the holiday. Additionally, if non-exempt, the employee shall receive time-and-one-half premium pay for all hours worked on such holiday.

5. Current University policies for recording holiday time remain applicable.

D. Recordkeeping

1. Alternative work Arrangements do not require any additional recordkeeping beyond what must already be kept pursuant to State and Federal law.

2. Alternative Work Arrangements for each employee, if implemented, should be communicated in writing to the employee and kept on file. The writing must identify the form of the Alternative Work Arrangement being implemented, the days of the week and the hours per day that the employee is required to work, the expected starting and ending times of the employee's workday, and any other pertinent information.

III. Telecommuting

A. Who May Telecommute

Exempt Managerial, Professional, Supervisory, and Confidential staff employees who have completed their probationary periods are eligible to be considered for telecommuting.

Not all eligible employees will be suitable for telecommuting. Suitability for telecommuting is based upon the individual employee as well as the employee's position.

B. Telecommuting Arrangements

Telecommuting shall only be scheduled as follows:

1. Regular: a recurring arrangement generally consisting of the same day or days each week when an employee works at the alternate location. Regular telecommuting arrangements can be for a finite or indefinite period of time.

2. Occasional (Non-Emergency): a sporadic occurrence from time to time, generally on an as-needed basis.

3. Emergency: telecommuting that is precipitated by a crisis or other emergency that significantly disrupts a facility or facilities or the physical operation of a department. When needed to achieve business continuity and to maintain critical functions, operations, and services, telecommuting arrangements may be established until normal operations can be restored at the regular work location.

   In all cases, telecommuting arrangements are revocable and can be discontinued at any time when it is in the judgment of the department that it is in the best interest of the university to do so. Departments should give 30 days' notice of discontinuance unless extenuating circumstances make such notice impracticable.

   Telecommuting does not change an employee's terms and conditions of employment, including required compliance with or the application of university policies. Additionally, an employee's compensation and/or benefits do not change as a result of a telecommuting arrangement.

   Telecommuting is not intended to permit employees to have time to work at other jobs or attend to other personal business, nor is it intended as a substitute for dependent care. If persons in need of primary care are regularly present in the alternate work location while the employee is telecommuting, the employee must demonstrate that another individual is present to provide the care.

   Telecommuting is not intended to circumvent any leave that an employee has requested and is entitled to pursuant to state and/or federal law, university policy, or prevailing collective negotiations agreements.

C. Work Site

The alternate location from which an employee telecommutes should be a predetermined site, such as a home office, and should have a fixed work area that will provide the employee with adequate access to the tools necessary for telecommuting, such as a telephone, computer, internet connection, etc.

A supervisor or other appropriate university official may arrange to visit the alternate work location when appropriate, to evaluate it for appropriateness prior to approving the telecommuting agreement or when worksite-related concerns arise during the telecommuting arrangement. Additionally, the university retains the right to make prearranged on-site inspections of the remote work site during scheduled work hours.

Telecommuters should not hold business visits or in-person meetings with professional colleagues, customers, or the public at alternate work sites; exceptions to this provision must be approved in advance by the department.

Telecommuting does not convert the alternate work location into a university place of business.

D. Costs and Expenses

All costs, whether relating to the initial set-up or the maintenance of a telecommuting arrangement, will be borne by the employee. The university does not assume responsibility for operating costs, home maintenance, or other costs incurred by employees in the use of their homes or other alternative work locations.

The university will not reimburse employees for out-of-pocket expenses for materials and supplies that are normally available at their regular work location.

E. Equipment

Except as set forth below, employees must provide their own computer, telephone, telephone service, internet connection, and any other equipment necessary to facilitate the telecommuting arrangement, unless otherwise expressly agreed to and approved. The university does not assume responsibility for the cost of employee-provided equipment or its repair or service.

Departments are not prohibited from using university funds for reasonable expenses that are necessary to facilitate the telecommuting arrangement, if there is a legitimate business need and adequate funding exists. Such expenses must be consistent with existing university policies regarding purchasing and business expenditures.

When available, departments are permitted to issue university-owned equipment to an employee for use in telecommuting; however, the equipment is to be used only by the telecommuting employee to perform authorized university business. When university-owned equipment is issued to an employee for telecommuting, the employee is responsible for protecting it from theft, damage, and unauthorized use. University-issued equipment used in the normal course of employment will continue to be supported by the department.

F. Accountability and Availability

In general, telecommuting should not change the regular days and hours that an employee is expected to be working; however, if a telecommuting employee will be performing work outside of the employee’s normal work days and hours, those work days and/or hours must be set forth in the Telecommuting Agreement. If it is found that an employee is not performing work during the telecommuting hours, the Telecommuting Agreement can be revoked, and the employee may be subject to discipline as appropriate.

A telecommuting employee shall be as available for communication and contact during the scheduled telecommuting time as he or she would be if working at the regularly-assigned work location. Where practical, supervisors should outline minimum expectations for how often the telecommuting employee should check email and voicemail.

A telecommuting employee shall report to the regularly-assigned work location on non-telecommuting days. In addition, supervisors may require that on a regular telecommuting day an employee must report to the regularly-assigned work location or elsewhere as needed for work-related meetings or other events. In that event, the supervisor should give the employee as much notice as is practicable.

G. Assessment

Certain adaptations may be necessary in how supervisors communicate expectations and assignments, and provide ongoing assessment and feedback, due to the fact that the telecommuting employee is not always physically present in the regular work location. The supervisor and the telecommuting employee should agree upon a workable means for delivering such information, such as regular meetings or status emails. Likewise, supervisors should also review and/or revise the criteria that will be utilized for annual performance appraisals where applicable. Such criteria should be clearly defined and measurable in terms of quantity, quality, or time to complete.

H. Process

A department can offer a telecommuting arrangement to a suitable employee or an employee may initiate a request to telecommute. In either case, the department should enter into a Telecommuting Agreement (http://uhr.rutgers.edu/sites/default/files/userfiles/TelecommutingAgreement.doc), only if it is determined that the employee and the employee’s position are suitable for telecommuting.

A Telecommuting Agreement may be discontinued at any time by either the employee or the department upon notice. Departments should give 30 days’ notice of discontinuance unless extenuating circumstances make such notice impracticable. The employee should give as much notice as is reasonably necessary to facilitate resumed reporting to the work location.

I. Risk Management

Workers compensation covers job-related injuries that occur in the course and scope of employment. For further information, contact the Office of Risk Management and Insurance.

J. Security and Technology

Telecommuting employees must adhere to the established standards and protocol relating to information protection, security, and technology. Failure to adhere to the standards and protocol may result in revocation of the Telecommuting Agreement and appropriate disciplinary action.

IV. Interpretation of Policy

Please contact the Office of Labor Relations for interpretations or assistance with this policy.

Rutgers Counter Proposal

May 14, 2019

NEW ARTICLE – TELECOMMUTING

1. Exempt URA-represented staff employees who have completed their probationary periods are eligible to be considered for telecommuting. Not all eligible employees will be suitable for telecommuting. Suitability for telecommuting is based upon the individual employee as well as the employee's position and the needs of the employee's department (Department).

2. Telecommuting shall only be scheduled as follows:

   A. Regular: a recurring arrangement generally consisting of the same day or days each week when an employee works at the alternate location. Regular telecommuting arrangements can be for a finite or indefinite period of time.

   B. Occasional (Non-Emergency): a sporadic occurrence from time to time, generally on an as-needed basis.

   C. Emergency: telecommuting that is precipitated by a crisis or other emergency that significantly disrupts a facility or facilities or the physical operation of a department. When needed to achieve business continuity and to maintain critical functions, operations, and services, telecommuting arrangements may be established until normal operations can be restored at the regular work location.

3. In all cases, telecommuting arrangements are revocable and can be discontinued at any time when it is in the judgment of the Department that it is in the best interest of the Department to do so. The Department will give 30 days' notice of discontinuance unless extenuating circumstances make such notice impracticable.

4. Telecommuting does not change an employee's terms and conditions of employment, including required compliance with or the application of university policies. Additionally, an employee's compensation and/or benefits do not change as a result of a telecommuting arrangement.

5. Telecommuting is not intended to permit employees to have time to work at other jobs or attend to other personal business, nor is it intended as a substitute for dependent care. If persons in need of primary care are regularly present in the alternate work location while the employee is telecommuting, the employee must demonstrate that another individual is present to provide the care.

6. Telecommuting is not intended to circumvent any leave that an employee has requested and is entitled to pursuant to state and/or federal law, university policy, or prevailing collective negotiations agreements.

7. Prior to executing a Telecommuting Agreement, an employee shall complete the Safety Self-Audit, review and sign the Information Technology Use Policy, and the Request to Telecommute form and attach said documents to the Telecommuting Agreement for approval by his/her

Rutgers Counter Proposal

May 14, 2019

supervisor. Prior to executing a Telecommuting Agreement, a supervisor shall review the documents referenced above for completeness and shall complete the Feasibility Assessment Telecommuting Policy form and have said form approved by his/her supervisor. Upon receipt of an executed Telecommuting Agreement from his/her supervisor, an employee shall execute and return the Telecommuting Agreement.

8. The alternate location from which an employee telecommutes should be a predetermined site, such as a home office, and should have a fixed work area that will provide the employee with adequate access to the tools necessary for telecommuting, such as a telephone, computer, internet connection, etc. A supervisor or other appropriate university official may arrange to visit the alternate work location, or have the employee provide electronic images if the supervisor deems such images are acceptable, when appropriate, to evaluate it for appropriateness prior to approving the telecommuting agreement or when worksite-related concerns arise during the telecommuting arrangement. The purpose of such a visit is to ensure compliance of the alternate work location with the conditions contained in the Telecommuting Agreement **and related** documents set forth in Paragraph 8 above. Additionally, the Department retains the right to make prearranged on-site inspections of the remote work site during scheduled work hours. Telecommuters should not hold business visits or in-person meetings with professional colleagues, customers, or the public at alternate work sites; exceptions to this provision must be approved in advance by the Department. Telecommuting does not convert the alternate work location into a university place of business.

9. All costs, whether relating to the initial set-up or the maintenance of a telecommuting arrangement, will be borne by the employee. The Department does not assume responsibility for operating costs, home maintenance, or other costs incurred by employees in the use of their homes or other alternative work locations. The Department will not reimburse the employee for out-of-pocket expenses for materials and supplies that are normally available at his/her regular work location. Where the work performed at the alternate location requires technology, equipment or supplies, such as hardware, software, paper, ink, or the like, that exceed the type or amount typical for home office use, the employee may request that the Department provide directly, or through lending, such technology, materials or equipment.

10. Except as set forth below, the employee must provide his/her own computer, telephone, telephone service, internet connection, and any other equipment necessary to facilitate the telecommuting arrangement, unless otherwise expressly agreed to and approved. The Department does not assume responsibility for the cost of employee-provided equipment or its repair or service. The Department may, at its discretion, use its funds for reasonable expenses that are necessary to facilitate the telecommuting arrangement, if there is a legitimate business need and adequate funding exists. Such expenses must be consistent with existing university policies regarding purchasing and business expenditures. When available, and at its discretion, the Department may issue university-owned equipment to an employee for use in telecommuting; however, the equipment is to be used only by the telecommuting employee to perform authorized university business. When university-owned equipment is issued to an employee for telecommuting, the employee is responsible for taking reasonable steps to protect it from theft, damage, and

Rutgers Counter Proposal

May 14, 2019

unauthorized use. University-issued equipment used in the normal course of employment will continue to be supported by the Department.

11. In general, telecommuting should not change the regular days and hours that an employee is expected to be working; however, if a telecommuting employee will be performing work outside of the employee's normal work days and hours, those work days and/or hours will be set forth by the Department in the Telecommuting Agreement. If it is found that an employee is not performing work during the telecommuting hours, the Telecommuting Agreement can be revoked, and the employee may be subject to discipline as appropriate.

12. A telecommuting employee shall be as available for communication and contact during the scheduled telecommuting time as he or she would be if working at the regularly-assigned work location. Where practical, supervisors will outline minimum expectations for how often the telecommuting employee should check email and voicemail.

13. If relevant to the type of telecommuting schedule assigned to the employee, the telecommuting employee shall report to the regularly-assigned work location on non-telecommuting days. In addition, supervisors may require that on a regular telecommuting day an employee must report to the regularly-assigned work location or elsewhere as needed for work-related meetings or other events. In that event, the supervisor should give the employee as much notice as is practicable.

14. Certain adaptations may be necessary in how supervisors communicate expectations and assignments, and provide ongoing assessment and feedback, due to the fact that the telecommuting employee is not always physically present in the regular work location. The supervisor and the telecommuting employee should agree upon a workable means for delivering such information, such as regular meetings or status emails. Likewise, supervisors should also review and/or revise the criteria that will be utilized for annual performance appraisals where applicable. Such criteria should be clearly defined and measurable in terms of quantity, quality, or time to complete. A supervisor who will be supervising a telecommuting employee must review the Managing Employee Performance Telecommuting Policy form prior to the employee telecommuting.

15. The Department may offer a telecommuting arrangement to a suitable employee or an employee may initiate a request to telecommute. In either case, the Department must enter into a Telecommuting Agreement if it is determined that the employee and the employee's position are suitable for telecommuting. An employee initiating a request to telecommute must do so by utilizing the Telecommuting Request form.

16. A Telecommuting employee must adhere to the established standards and protocol relating to information protection, security, and technology as set forth in, but not limited to, the Remote Site Security Standards. Failure to adhere to the standards and protocol may result in revocation of the Telecommuting Agreement and appropriate disciplinary action.

17. Except where the provisions therein are inapplicable or are in conflict with the provisions contained in this Article, the University Human Resources Telecommuting Guidelines shall apply

Rutgers Counter Proposal

May 14, 2019

in all instances whereby a URA-represented employee of the Department is telecommuting. A copy of the guidelines will be furnished to the URA-AFT unit member prior to executing the Telecommuting Agreement.

18. No employee shall begin telecommuting prior to executing a Telecommuting Agreement with the Department.

19. Except where the provisions therein are inapplicable or are in conflict with the provisions contained in this Article, University Policy 60.3.22 shall apply in all instances whereby a URA-represented employee of the Department is telecommuting.

20. Determinations of the Department as to whether an employee may telecommute shall be final and not subject to the grievance procedure.

5/29/19

5|29|19

RUTGERS
University Human Resources

TO COMPLETE THIS FORM, DOWNLOAD THE .DOC VERSION

Safety Self Audit
Telecommuting Policy

This form lists areas and items the employee must inspect before telecommuting begins to ensure that the designated Alternate Work Location is safe, ergonomically suitable, and free from hazards. The employee and his or her supervisor may add items to the list as needed. For additional information regarding working safely, you may contact Rutgers Environmental Health and Safety at 732-445-2550.

Once the checklist is completed, the employee must share it with his or her immediate supervisor for review and discussion.

Name of Telecommuter: ____________________________________ Unit: ____________________________________

Alternate Work Location:____

Employee: Review the following list and indicate the status of each item. Your supervisor may list other items to review as they are related to your assigned tasks. Once complete, share the list with your immediate supervisor to discuss the safety of the alternate work location, whether it is appropriate for telecommuting, and if changes need to be made.

Safety Items to Review	Yes	No	Unsure
Is the workstation arranged to be comfortable without unnecessary strain on back, arms, neck?	□	□	□
Are cords, cables, or other items arranged to prevent a tripping hazard?	□	□	□
Is the lighting adequate for assigned tasks?	□	□	□
Are there provisions in place to adequately secure equipment and data?	□	□	□
Is the workspace kept clean from trash or other combustible materials?	□	□	□
Are three-wired grounded outlets or circuit breaker power strips used?	□	□	□
Is the work area separate from major home activity areas?	□	□	□
Is the work area void of background/distracting noise during work hours?	□	□	□
____	□	□	□
____	□	□	□
____	□	□	□
____	□	□	□
____	□	□	□

RUTGERS
THE STATE UNIVERSITY
OF NEW JERSEY

UNIVERSITY POLICY

Policy Name:	Acceptable Use Policy for Information Technology Resources				
Section #:	70.1.1	**Section Title:**	Information Technology	**Formerly Book:**	N/A
Approval Authority:	Executive Vice President for Finance and Administration and University Treasurer	**Adopted:**	2/1/2000	**Reviewed:**	12/13/2018
Responsible Executive:	Senior Vice President and Chief Information Officer	**Revised:**	08/31/2010; 01/23/2013; 10/10/2013; 07/03/2014; 10/27/2014, 08/22/2016; 02/27/2017 *(Reverted back to 10/27/2014 version)*; 12/13/2018		
Responsible Office:	Office of Information Technology (OIT)	**Contact:**	oitpolicies@rutgers.edu		

1. Policy Statement

It is the policy of Rutgers University to allow access for its community to local, national, and international sources of information and to provide an atmosphere that encourages the free exchange of ideas and sharing of information. Nevertheless, Rutgers reserves the right to limit or restrict the use of its information technology resources based on applicable law, institutional policies and priorities, and financial considerations. Access to the University's information technology resources is a privilege that requires each member to act responsibly and guard against inappropriate use and abuse. Therefore, both the community as a whole and each individual user have an obligation to abide by the following standards of acceptable use.

Users' expectations of privacy protection for electronic data must be balanced against the University's reasonable need to supervise, control, and operate the University's information systems. Although the University will not monitor the content of electronic documents or messages as a routine matter, it reserves the right to examine all computer files and content in order to protect individuals and the University.

2. Reason for Policy

This policy outlines the acceptable use of University information technology resources, which include, but are not limited to: equipment, software, networks, systems, data storage devices, media, facilities, and stationary and mobile devices used to access Rutgers information technology resources, whether the technology or devices are personally owned, leased, or otherwise provided by Rutgers University. Information technology resources also include any and all Rutgers data, records, information, and record systems stored on or retrievable from such equipment, software, networks, systems, data storage devices, media, and facilities, or stationary and mobile devices.

3. Who Should Read This Policy

All members of the Rutgers University community.

4. Resources

University Policy: Information Technology - Section 70: https://policies.rutgers.edu

University Policy: Clinical, Compliance, Ethics & Corporate Integrity - Section 100: https://policies.rutgers.edu

University Policy 50.3.7: Copyright Policy

University Policy 70.1.6: Email and Calendar Policy

OIT Policies Website: http://oit.rutgers.edu/policies

RU Secure Website: http://rusecure.rutgers.edu/

5. Definitions

N/A

6. The Policy

A. User Responsibilities

Because the primary use of the University's communications and business systems is to further the institutional mission, members of the University community should not have the expectation of privacy in their use of electronic systems, whether work-related or personal. By their nature, electronic systems may not be secure from unauthorized access, viewing, or infringement. Although the University employs technologies to secure its electronic resources, as a rule confidentiality of electronic data cannot be assumed.

i. **Each user may use only those information technology resources for which he or she has authorization. Violations include but are not limited to:**

- using resources without specific authorization
- using another individual's electronic identity
- accessing files, data, or processes without authorization

ii. **Information technology resources must be used only for their intended purpose(s). Violations include but are not limited to:**

- misusing software to hide personal identity, or to interfere with other systems or users;
- misrepresenting a user's identity in any electronic communication;
- using electronic resources for deceiving, harassing, or stalking other individuals. University Policy 60.1.12: Policy Prohibiting Discrimination and Harassment;
- sending threats, "hoax" messages, chain letters, or phishing;
- sending mass emails to the Rutgers community without following proper procedures;
- intercepting, monitoring, or retrieving without authorization any network or other electronic communication;

- using University computing or network resources for private advertising or other private commercial purposes. https://oit.rutgers.edu/official-email;

- circumventing, disabling, or attempting to circumvent or disable security mechanisms without authorization;

- using privileged access to University systems and resources for other than official duties directly related to job responsibilities, with the exception of incidental private use;

- making University systems and resources available to those not affiliated with the University;

- using former system and access privileges without authorization after association with Rutgers has ended or using system and access privileges to a former department's resources without authorization after the transfer to the new department.

iii. The access to and integrity of information technology resources must be protected. Violations include but are not limited to:

- Using third party, cloud and non-cloud, systems not authorized or approved by OIT's Information Protection & Security Division to transmit, process, or store Rutgers data classified as restricted. University Policy 70.1.2: Information Classification;

- creating or propagating computer viruses, worms, Trojan Horses, or any other malicious code;

- preventing others from accessing an authorized service;

- developing or using programs that may cause problems or disrupt services for other users;

- degrading or attempting to degrade performance or deny service;

- corrupting or misusing information;

- altering or destroying information without authorization.

iv. Applicable state and federal laws and University policies must be followed. Violations include but are not limited to:

a) Laws

- failure to respect the copyrights and intellectual property rights of others;

- making more copies of licensed software than the license allows;

- downloading, using, or distributing illegally obtained media (e.g., software, music, movies);

- uploading, downloading, distributing, or possessing electronic content explicity prohibited by federal, state, or local law (i.e., child pornography)

b) Policies

- accessing, storing, or transmitting information classified as Restricted (e.g., social security numbers, patient health information, driver's license numbers, credit card numbers) without a valid business or academic reason or transmitting such information without using appropriate security protocols (e.g., encryption). University Policy 70.1.2: Information Classification and https://rusecure.rutgers.edu/data-classification;

- distributing data/information classified as Restricted, unless acting as an authoritative University source and an authorized University distributor of that data/information and the recipient is authorized to receive that data/information;

- using social media to communicate or store University data/information classified as Restricted;

- using third party cloud storage or data sharing tools (i.e., iCloud, Carbonite, Dropbox) to store University information classified as Restricted.

v. **University business should be conducted using University provided information technology systems, resources, and services.**

vi. **Accessing information and Records:** Recognizing that not all circumstances can be anticipated, access to information and records residing on University information technology resources will ordinarily be governed by the following:

a) **University Responsibilities:** The University's obligations in relation to information technology resources include ensuring compliance with applicable laws and University policies and procedures, protecting the integrity and operation of its resources, and preserving information as necessary to protect the interests of the University and to enable it to satisfy these obligations. Accordingly, the University may access Rutgers-related electronic information on any device on which it is stored or may be accessed, and may access a user's records and information stored on University information technology resources systems or equipment for the above-mentioned purposes. Such access must be for specific, articulable reasons, must be appropriately circumscribed, and is limited to authorized personnel. The University understands that some users may have personal information and/or records on University systems and it respects the privacy of all users as to such information insofar as possible in complying with its above-mentioned obligations.

i. Standards for Accessing or Monitoring Information and Records: The University may access or monitor any/all information, records, record systems, and/or information technology resources in the following circumstances:

1. As necessary or appropriate to avert reasonably anticipated or already apparent threats or hazards to University information, records, or information technology resources. An example includes scanning to detect computer viruses;

2. As and when required by law or to comply with legal or contractual obligations of the University;

3. In connection with a legal proceeding in which the Office of General Counsel is involved or an investigation conducted by or on behalf of

the Office of Employment Equity or University Ethics and Compliance, for which access is necessary or appropriate;

4. When there is reasonable cause to believe that the employee has engaged in misconduct, has violated University policies or regulations, or may have used University resources improperly and that the information and records to be accessed or monitored are relevant to the misconduct or violation in question;

5. When the University otherwise has a legitimate need to access the information, records, or information technology resources.

   Reasonable efforts will be made to notify the individual of the need for access to information or records in which the individual has a substantial personal interest in information or records stored on or transmitted through the University's information technology resources or other electronic system unless prohibited by law, inconsistent with University policy, or inconsistent with the University carrying out its normal operations and/or aforementioned obligations.

ii. Preserving and Protecting Records: In circumstances where the University determines that there may be a specific risk to the integrity or security of records, data, information, or information technology resources, the University may take measures to protect or preserve them. For instance, the University may take a "snapshot" of a computing account to preserve its status on a given date, copy the contents of a file folder, or restrict user access to information technology resources in whole or in part.

b) Employee Obligations

i. Standards of Employee Conduct for Accessing or Monitoring Records: It is a violation of this policy for an employee to monitor information technology resources or record systems or access records beyond the standards established within this policy. It is also a violation of the policy if the University has granted access to the employee (to monitor or access records or systems) and the employee has accessed or monitored records or record systems for purposes other than the purposes for which the University has granted access.

B. Violations

Employees who violate this policy may be subject to relevant institutional sanctions and discipline up to and including termination of employment.

RUTGERS

School of Communication and Information
Rutgers, The State University of New Jersey
4 Huntington Street
New Brunswick, NJ 08901-1071

comminfo.rutgers.edu
Phone: 848-932-7500
Fax: 732-932-6916

Policies Related to Purchases, Support, and Protection of Hardware, Software, Data, and Technology Services

Last updated April 30, 2019

The School of Communication and Information supports the technology needs of its faculty and staff in the performance of teaching, research, administration, and other job responsibilities. In many cases SC&I provides the infrastructure, hardware, software, and IT services that are needed by departments, programs, and individuals in the school to accomplish goals related to the mission of the school. We also assist those who have particular IT needs to help them select the appropriate technology tools, and either provide support, or advice in finding support, for technologies that they choose to adopt.

A key principle for the school's information technology function is that it should be value-added; we strive not to duplicate technology or services that the university provides. Because of the innovative research and teaching methods in use at the school, SC&I often adopts technologies in advance of the university (email about six years before the university, VoIP phone service about ten years before the university, lecture-capture several years before the university), but when the university later adopts technology with similar functionality, our practice is to participate in the university system and focus our limited efforts on services only we can provide.

The IT Services website at http://its.comminfo.rutgers.edu provides details about the technology and services offered by the school.

This policy outlines the principles and practices used by the School of Communication and Information in providing hardware, software, and services. While we attempt to support the widest range of hardware and software possible, staffing and other resource constraints mean that there are limits to our operations and support.

PURCHASE OF TECHNOLOGY

All hardware purchased with university funds must be tagged for inventory purposes. This applies to items purchased through IT Services, faculty support staff, purchase order, or expense reimbursement.

All devices, excluding phones and tablets, purchased through SC&I IT Services must be configured so that the IT office has an administrative account on it to assure the device meets compliance and security requirements at Rutgers.

Staff: The school provides from its central resources a computer, two monitors, and a desktop printer to each full-time staff member. In general there are standard models and set-ups available, with small individual preferences allowed. When there is a business case for a staff member to be assigned a laptop computer, such as when the position must routinely work from locations outside SC&I, the school will provide the laptop. Computers, monitors, and printers for part-time staff are addressed on a case by case basis. Any optional equipment a staff member needs or wants such as headphones, speakers, tablets, cameras, or webcams, comes from the departmental budget and therefore must be discussed with the supervisor. Those equipment purchases must be made with the consultation of IT Services as well.

Full-time faculty: Faculty members are provided with start-up and annual support funds so they can purchase the desktop and laptop computers, printers, and accessories they need for their work. Faculty may have other university support funds with which to purchase equipment as well, such as funds from teaching a Byrne Seminar, and may also have external funding that allows such purchases. Faculty discuss their technology needs with IT Services, who then obtain quotes for all non-consumable equipment. Upon faculty approval of a quote, ITS coordinates with the Business Office to have the order processed and charged to the appropriate faculty financial accounts. As with staff equipment, ITS receives the items, reviews them, adds them to an inventory list, affixes asset tags, and configures, secures, and sets up the equipment.

It is not possible for IT Services to support every brand and model of every computer, monitor, or printer. Faculty who choose to purchase unique hardware may be asked to acknowledge in writing at the time of purchase that there may not be support from IT Services for that hardware.

It is understood that sometimes equipment purchased with university funds may be used by a faculty member at home. If the purchase was made through IT Services, the helpdesk will provide support for that equipment, but it may need to be brought into SC&I in order to be serviced. All such devices and software are expected to be maintained in compliance with system and security standards of the school. Note that supplies for such equipment – such as ink cartridges for home printers – are charged to a faculty member's support funds rather than the school's IT Services budget.

Faculty who need non-computer equipment such as cameras to teach a class should work with their chair, the program director, and the program faculty to agree on adoption of such equipment appropriate for everyone who teaches that particular course. The school is in the process of determining staffing and best practices for support of audio-visual equipment given the curricular expansion requiring such material.

Centers, labs, work groups: Faculty who work in designated centers or labs, or who work in research groups with students formally or informally, generally use their support funds or external funds to procure any equipment needed for those students. As with other purchases, IT Services should be involved when hardware and software is being ordered to assure the items meet system and security standards, can be supported through normal use, and are processed through IT Services upon arrival.

When a faculty member is submitting a grant that will require significant hardware or software, IT should participate in the work plan to assure the project can be supported successfully. When an externally funded project makes use of information technology and services such as web design, website hosting, application development, or system administration beyond what the school generally provides, or has significant needs for resources such as bulk printing, the school will work with the group to consider the most appropriate work plan and financial model. The school will work with the Office of Advanced Research Computing when that is possible and appropriate. IT Services continually assesses the needs of the school and makes recommendations to the Dean's Office about new staff, technology, and services that the school should be providing to meet faculty and research team needs.

Part-time faculty and doctoral students: Part-time faculty and doctoral students share several common spaces around SC&I buildings, and the school provides a small number of computers, monitors, and printers to be shared in those spaces. The computers are typically the same as those in the school's computer labs:

they do not allow data to be saved to the hard drive in order to prevent viruses and misuse, and they are set up to assure connectivity to the wired network and to printers.

If a part-time faculty member is teaching a class that requires specialized software, and the department has agreed to the adoption of that software, the school will provide a copy/license of that software to the individual.

Personal devices: SC&I cannot be responsible for servicing personal devices, defined as devices purchased with non-university funds. Any faculty or staff member who brings their personal equipment to use at SC&I may not be able to access the SC&I network and/or school services. Through use of a NetID, the device may be able to get on RU Wireless and access services available on the web, but it may not be able to print to school printers or access other services. The school will not provide wired access to a personal device on our network, and we cannot install certain software packages available through the university that have exclusions of non-Rutgers devices. Personal computers will not be able to join the SC&I domain or access shared drives; to access shared drives those devices would have to VPN into a SC&I computer, if allowed.

A particular issue related to personal computers is their use for instruction in classrooms. Individuals who expect to connect a personal device to a classroom podium will need to provide their own adapter to connect. The large number of adapters in the marketplace (the many different types, and generations of each type) means that than the school cannot keep all of them on hand; even when some adapters were kept by the helpdesk, they were so often not returned that it is not possible for the school to provide this service.

The university makes some software available for download to personal devices as well as university devices, and all employees are encouraged to make use of this resource.

Classroom technology: In cooperation with Digital Classroom Services, SC&I supports the dedicated equipment in each school classroom. Support of classroom technology is by university policy the highest priority; anyone teaching in a classroom can and should expect working equipment in that room and should call IT Services immediately if there is a problem. However, as outlined above, IT Services cannot support personal computers that are connected to classroom podiums. Instructors should plan to use a flash drive, upload material to the web or cloud service, or make other arrangements to use the podium computer when teaching a class.

The podiums in general purpose classrooms are by policy not modified, since they are supposed to remain all the same. Podiums in SC&I-controlled classrooms, especially computer labs, may have additional software made available when needed for instruction. IT Services puts out a call in advance of each term for such requested upgrades and must coordinate sometimes conflicting requests as well as possible.

For all information technology at SC&I: IT Services must maintain physical and electronic access to all equipment, even equipment being used by research groups, to assure compliance with security requirements and Rutgers' acceptable use policy.

If a device is purchased through personal funds and submitted for expense management, the university will not reimburse for insurance or extended warranty for that device. If a device is purchased through a university purchase order, the university can cover optional warranty for extended battery protection and accidental damage. The school requires such optional coverage for a laptop, tablet, or other device that is mobile.

PURCHASE AND USE OF MOBILE DEVICES AND MOBILE DEVICE DATA PLANS

There may be cases when a faculty or staff member can make a business case for having a Rutgers-owned mobile phone and data plan to support his/her work. Typically such an individual would have responsibilities that involve extensive off-hours and/or off-campus work. If the case is approved, a faculty member would be using support funds and a staff member would be using departmental funds for the purchase.

In these cases, a phone and data plan will be obtained through the university purchasing system and 100% of the device and service plan would be covered through the purchase order. The device and phone number then belong to Rutgers but are assigned to the individual for their use; the device has university-required security on it, and remains with SC&I should the individual leave the university. SC&I IT Services does not provide support for the cell phone hardware.

Faculty members who wish to use their support funds to purchase a pad or tablet device may arrange such a purchase through the IT Services staff using a purchase order. As with laptops, the annual support may cover the full cost of the device. Faculty who also wish to purchase a data plan may present a business case to have that included on the purchase order. Staff members may be approved for a device to be purchased by their departments, as appropriate for their job responsibilities.

Faculty members who travel internationally for work can be reimbursed from their school support funds for international data plans on either school-owned or personal phones that allow them to maintain their regular level of work-related connectivity while traveling.
An employee who would like to use an email app on a mobile device to access Rutgers email must comply with the university's Mobile Device Management Policy. (See https://oit.rutgers.edu/connect/using/mdm-policy) It is possible to access email through a web browser as well.

(The school's previous IT policy offered an additional possibility which is now no longer being allowed. The previous policy allowed faculty members who used their personal cell phone for Rutgers business to use their annual support funds towards the purchase of a personal cell phone and submit for partial reimbursement of the device itself but not the voice/data plan. Up to 80% of the cost of the device could be reimbursed from the faculty member's support funds, up to a maximum of $500 (in keeping with university expense reimbursement policy). Senior staff members who regularly worked outside of the school's usual office hours or off-campus could also request reimbursement for up to 80% of a personal mobile device. This is no longer being allowed in accordance with practices across the university. The technology landscape has changed since the last policy was implemented. A similar evolution occurred when Internet access first became available. Initially the university would cover an Internet access plan for a faculty member's home, but no longer does so.)

SUPPORT FOR AGING HARDWARE

As communication and information technology ages, it requires increasing amounts of helpdesk support. At a certain point, an individual's desire to maintain an old piece of equipment conflicts with the amount of time IT staff can provide to that individual.

If a device or its operating system are no longer being supported by the vendor that manufactured it, it means the vendor is no longer providing security patches for that item and the device becomes a security risk to the school. The school will remove such devices from all university networks, and will notify the individual that the school can no longer support the device.

If a device is still being supported by the manufacturer but is beyond its expected useful age or has had extensive wear, over time it becomes very challenging to support. In these cases, the school reserves the right to notify a faculty or staff member that the device can no longer be supported.

IT staff work with individuals to help determine if the standard warranty period for a device is appropriate or a longer period should be added at the time of purchase. In general the warranty periods and useful lifetimes of devices are:

- Desktop computers: a standard warranty may be three to four years, useful life is about four to five years
- Laptop computers: standard warranty may be three to four years, useful life varies wildly based on use and care, but average may be about four years
- Tablet computers: standard warranty may be up to 90 days, useful life can be five years depending on use and care
- Cell phones: standard warranty may be up to two years, useful life may be three or four years, but note that IT Services does not support the cell phone hardware

PURCHASE AND LICENSING OF SOFTWARE AND TECHNOLOGY SERVICES

Rutgers University makes available a wide variety of software and technology services that serve the teaching, research, and administrative needs of employees. In addition, the university negotiates for discounts for other software and services that SC&I benefits from. The school uses centralized funds to procure software and technology services for faculty and staff when the software and services are critical to deliver the overall administrative services and teaching/educational mission of the school. The provision of such items is generally by purchasing copies of software or licensing with a vendor for the number of users required.

Academic programs and the teaching mission: The school asks each academic program to determine the software and services required for teaching its classes. Individual faculty decisions about the needs for particular classes should be approved by the program faculty as a whole to assure that the school is not asked to purchase different software for different sections of one class being taught by several people. When a part-time lecturer or PhD student is teaching a class, we will provide them with a copy of the approved software and, when appropriate, install copies of it on all computer lab machines. Students will have to purchase or license the software as they would a textbook.

IT Services and Instructional Design and Technology Services should be included in the discussion about technology to be adopted by programs. They are aware of academic and Rutgers-negotiated discounts available for particular products which may affect the decision making. They also need to understand what levels of support are required by students in those classes. If a technology is adopted for a class that IT Services is not able to support, they can work with the department to outline alternatives.

The school will also centrally procure software and services that underpin the research needs of a critical mass of faculty. In some cases such as Nvivo and Qualtrics, we pay into a university pool and everyone is entitled to access them. When faculty need other software and technology services for their particular research needs, they should discuss with IT Services to see if there is a university license that they or the school can access. When the school does not provide the software or license, the faculty member should use the support funds provided to them by the school and make the purchase through university procurement whenever possible. IT Services will work with the faculty member to either provide support or identify alternate means of supporting the software use.

Rutgers University has contracts and discounts available for a wide variety of software and services that help offset costs for many purchases. To access these contracts and discounts, items must be purchased through the university and not through expense reimbursement.

If faculty or staff purchase software that is not supported by IT Services, the approver of the purchase order or expense reimbursement will ask that individual sign an acknowledgement that the school does not provide support for that item.

[Future development of this policy should address student use of software.]

Software Request Guidelines for Faculty and Instructors

- Read SC&I's "Policies Related to Purchases, Support, and Protection of Hardware, Software, Data, and Technology Services"
- Review the technology services available to SC&I instructors and their students at http://go.rutgers.edu/1y3wc2hh
- Discuss software teaching needs with your department chair, program director, and colleagues
- All software requests must be approved by the department/program before being submitted
- Validate that funds are available for the purchase

Please consult with IT Services and IDTS in formulating your requests. All requests are subject to their approval.

Online Request Form: To request that the school installs software, complete the form at: https://goo.gl/forms/mW5mkyZBlKYuTjJb2 which asks for the following information:

- Course Title
- Course Number
- Name of instructor(s)

- The approximate number of students who will be using the software, including your class and any other classes that would potentially access it.
- Is this class approved as part of the campus core requirement? ___yes ___no
- List the number of legal copies (standalone, site license) needed.
- Provide the name of the software application with vendor and pricing information (including upgrade info).
- For which computer lab is this software intended? (CI-114A, CI-114B, CI-119, CI-222)
- How often will the software be used? (e.g., once a week for 20 person class for two semesters, or used by all courses scheduled in CI-119 at least once a week)
- Are there any special hardware, disk space, or network requirements needed to support the software?
- Is the software available in other labs on campus? See the following for lab software at Rutgers: http://go.rutgers.edu/6zc5pjk2
- Is an academic and/or student version of the software available?

Deadlines for Requests

- For use in the fall term: request by June 1
- For use in the spring term = request by October 1
- For use in the summer term = request by March 1

Requests submitted after the deadline may not be available for the start of the specified term.

Request Review Process

- Requests related to upgrades of existing applications as well as new software should be submitted via the application process described above.
- Priority will be given to requests that benefit the greatest number of students in coursework and for which there do not exist good substitutes already on campus.
- A subcommittee of IDTS and ITS will review requests and analyze based on
    - Total cost
    - Legality – whether the software can be used in a lab setting
    - Technical feasibility – whether the software is compatible with the school's hardware and other installed software
    - Logistics – whether there are course scheduling issues or other issues related to the installation

Notification

- Departments and faculty will be notified via email when the software is being obtained or if there is a problem with implementing it.
- If IT Services and IDTS determine there are problems implementing the software, a meeting will be scheduled to discuss with the chair and faculty member to find a solution to the technology need.

Instructor Responsibility

- The instructor should plan to test the software after it is installed in the labs before the start of classes.
- IT Services and IDTS cannot provide training or support for special software. We strongly advise instructors to provide their own training for the software to their students and/or utilize resources such as Lynda.com for this purpose.
- Instructors who need assistance in creating software training materials for students should contact IDTS (sci-idts@comminfo.rutgers.edu).

TECHNOLOGY REPLACEMENTS AND UPGRADES

Inventory is kept of all devices purchased with university funds, whether purchased through a purchase order or expense reimbursement.

When a replacement device is purchased, faculty and staff will be asked to return the old device to IT Services unless the old device will be in continued use. In cases of software and licenses for which someone is entitled to just one instance, the software or license will be migrated from the old to the new device. However, some cloud-based software purchases/licenses allow for use by multiple devices by a single user which may make it possible to retain the old device and have it retain its full use. Both devices are still owned by Rutgers and must be returned when no longer in use.

If someone loses or damages a university-owned device as a result of their own inadequate measures to prevent theft or damage, the school will not pay to replace the device.

DISPOSITION OF TECHNOLOGY WHEN SEPARATING FROM THE UNIVERSITY

All equipment and software purchased with Rutgers funding is the property of Rutgers University. An employee in possession of any electronic device, software copy, or license for software or service made with Rutgers funds - whether through a purchase order or expense reimbursement – who leaves Rutgers will generally be given the opportunity to either purchase the item from the university at resale value or return the item to the school. Any software that was made available to the employee on a device he/she purchases from the school will be removed before the resale to the employee unless arrangements for purchase of that software or license are explicitly made and as long as the software is permitted on equipment not owned by the university.

LOANER EQUIPMENT

The school maintains some equipment which can be loaned out to a faculty or staff member when their regular devices are being serviced and in case of other short-term urgent needs.

Registered student organizations may borrow equipment for hosting hybrid meetings, request posters for hosted events, ask for lecture capture or videotaping of events. Working with the Office of Student Services, IT Services will provide an orientation to any student organization to explain services and support generally available, will provide loaner equipment if the group requests items that are available, and will provide other support on a case-by-case basis as possible.

SENSITIVE DATA

Research Data

Researchers who collect sensitive data from or about human subjects must abide by the terms outlined in their IRB-approved research protocol. IT Services will work with researchers to assure that their electronic data is secured as required.

Protected Health Information

SC&I staff are not trained or positioned to appropriately handle Protected Health Information (PHI) data even if the requestor is comfortable with asking for help from IT Services, and will therefore avoid handling files that include such data.

Non-Public Personal Information

SC&I cooperates with the university in assuring security for personal data and Non-Public Personal Information (NPPI) held on any university device or database. Our policy and strategies outlined below either duplicate or augment university policies regarding such information.

Important Definitions

<u>Non-Public Personal Information (NPPI):</u> As outlined by Rutgers University Policy 70.1.2, NPPI includes but is not limited to:

- Social Security numbers
- Driver’s license numbers or state identification card numbers
- Credit or debit card numbers
- Medical records
- Student records
- Financial records
- Legal Records
- Police Records
- Studies or surveys using confidential or personally identifiable date
- Birth Date

University departments should not collect or use a Social Security Number, with the exception of temporary use to process a new employee. Employees can be identified through their Employee ID number from the university’s HCM personnel system, and students can be identified through use of the RU ID.

Classification of Data: Classifications are helpful in determining the level of risk involved related to various forms of data. Rutgers uses three classifications.

Restricted Data (highest level of sensitive): Restricted Data is the most sensitive information and requires the highest level of protection. This information is usually described as "non-public personal information (NPPI)" and is related to people or critical business, academic, or research operations under the purview of the Owner/Data Custodian. Restricted data includes, but is not limited to, data that Rutgers is required to protect under regulatory or legal requirements. Unauthorized disclosure or inappropriate use of restricted information could result in adverse legal, financial, or reputational impact on the university. Examples of Restricted Data include but are not limited to: sensitive student or employee identifiable information (i.e., Social Security Number, driver's license number, etc.), credit card information, confidential research, and file encryption keys, as well as certain financial records, medical records, legal records, student records, police records.

Limited Access Data: Limited Access Data is information that does not meet the requirements of restricted data but requires a moderate level of sensitivity and protection from risk and disclosure. Limited Access Data is the default and should be used for data intended for use within the university or any of its units with a legitimate need-to-know. Limited Access Data may be information one unit decides to share with another outside their administrative control for the purpose of collaboration. Unauthorized disclosure or inappropriate use of Limited Access Data could adversely impact the university, individuals, or affiliates but would not necessarily violate existing laws or regulations. Examples of Limited Access Data include but are not limited to: incomplete or unpublished research, internal memos or reports, personal cell phone numbers, project data, data covered by non-disclosure agreements. Although most Limited Access data is not technically NPPI, in many cases, we will agree to protect it in the same manner in order to comply with the security requirements of organizations providing data as part of grant requests. In addition, if there is any concern that limited access data should be better protected, please contact the Information Technology Services group for assistance or guidance.

Public Data (low level of sensitivity): Public Data is information that may or must be open to the general public. It is information with no existing local, national or international legal restrictions on access or usage. Public data, while subject to university disclosure rules, is available to all individuals and entities both internal and external to the University. While the requirements for protection of public data are less than that of Restricted and Limited Access Data, sufficient controls must be maintained to protect data integrity and unauthorized modification or destruction. Examples of Public Data include but are not limited to: data on websites intended for the general public, course listings, press releases, marketing brochures, university maps, and annual reports. Typically, we do not protect any public data with NPPI restrictions or protections, nor are individuals required to register as a data custodian for the use of public data. If public data has been used to create new information that has value, then that information should be protected by centrally storing it on our systems within SC&I.

Data Custodian: A data custodian is anyone who has access to, stores, transmits, or uses NPPI at SC&I. This includes restricted data and limited access data that is being protected as restricted data for the purposes of grant requests or in order to provide better protection on that data.

Protecting Restricted and Limited Access Data

Everyone responsible for creating, storing, or transmitting sensitive information is required to do so in a manner which protects NPPI. Any breach of security or compromise of systems containing NPPI must be reported immediately to the Office of Information Protection and Security (IPS) (rusecure.rutgers.edu) and the SC&I Dean's Office.

Hardcopy records of personal information (e.g. paper payroll documents, DVD's or tape backups with personal information) should be kept in locked cabinets, behind locked doors. Protected hard copy data should be shredded as part of the disposal process. If there is a need to send these records to another department or external agency, the documents should be sent in a sealed envelope or other packaging, marked confidential, and addressed to a specific recipient. NPPI should never be sent via email unless encrypted.

Anyone maintaining personal information in electronic form must strictly control access by encrypting the information. Where the information is limited access and protected through passwords rather than encryption, passwords should be complex and never shared. Due to the vulnerability of information on portable/mobile devices such as laptops, external hard drives, or USB memory sticks, restricted and limited access information on these devices should be encrypted.

Cell phones and tablets with sensitive information should utilize additional security measures such as strong access codes, disabling location services, time-out screen locking, and account lockout and/or remote wiping. University data housed on portable devices (laptops, cell phones, tablets, pen drives, etc.) or transmitted to and/or stored on "cloud services" should be encrypted with the encryption key separate from the device.

Travel with electronic devices requires special precautions. Remote devices and the information they contain should be protected while accessing the Internet or not physically under the owner's control.

Because of the risks when using cloud or third party providers, anyone using such services must discuss their storage of sensitive information with the Assistant Dean for Information Technology before storing such information with a third party.

The Information Technology Services office in conjunction with the SC&I Dean's Office is responsible for managing and acting as the data custodian for these different data types in the school. Appropriately safeguarding and managing this data is a primary function of the ITS office. As primary data custodians for the school, the ITS office will identify, classify, and protect NPPI and the systems the data resides on. The ITS office will periodically scan all systems for NPPI, identify those systems with it, perform risk assessments, ensure compliance, and train users on security best practices.

Members of the School of Communication and Information community are required to know what constitutes NPPI. In addition, if an individual meets the criteria for being deemed a data custodian, that individual should:

- Register as a data custodian with the School of Communication and Information. All registered data custodians will be included in a database for tracking sensitive information usage at SC&I. Anyone who meets the criteria of a data custodian whether an employee, student, or affiliate member must register immediately upon becoming a data custodian.
- Maintain NPPI in a dedicated, centralized, and secured location.
    - Electronic information should only reside on dedicated file servers (networked drives) within the SC&I environment.
    - Hard copy information should be stored in locked drawers or filing cabinets when it is not being used. When such sensitive information is being used, the material should not be left unattended, nor should any such information be left in a room that is unlocked. The information should not be left outside of its primary storage location overnight.
- Not store electronic NPPI on local systems, portable systems, portable devices, or systems being used for remote access to the SC&I networks.
- Not store or transfer NPPI using university or personal email accounts.
- Not transport hard copy NPPI outside the confines of the school or center in which it is being held.
- Not publish NPPI to web sites or any internal or external file sharing systems other than the dedicated SC&I file sharing servers. This includes files sharing systems like drop box and replication systems like iCloud or Dropbox.
- Not take any NPPI with them should they no longer be employed by, or no longer be associated with SC&I.
- Appropriately discard unused/unnecessary NPPI as soon as possible by complying with the procedures outlined below under "Secure Removal and Disposal of NPPI."
- Notify Information Technology Services immediately if there are any possible threats related to the compromise of NPPI. This includes any security threats to computer systems using NPPI. For hardcopy information, this includes any possible breach of physical security to the locations where NPPI stored.
- Not remotely access NPPI on the secure servers at the SC&I through a VPN connection if they have any suspicion that the machine being used to connect to the information is infected with malware, spyware, or a computer virus.

Should it become necessary to store NPPI outside the parameters set forth in this policy, an exception request must be completed by the appropriate data custodian and, where necessary, be approved by the Dean's Office prior to the data leaving the School as listed below. This provision allows the Dean's office to provide the requestor with advice on best practices for ensuring additional security measures are taken to protect the sensitive information.

User Responsibilities

Data custodians are responsible for storing all sensitive information on the designated systems within the technical environment of the School of Communication and Information. The protection of these systems and the associated internal networks are the responsibility of the Information Technology Services staff. If an individual is using sensitive information based on an exception request, then that individual is responsible

for the safety and security of that data. Data custodians are expected to notify IT Services (for electronic information) or the Business Office (for hard copy information) immediately if any threats arise that may jeopardize the security of NPPI. It is also expected that any individuals acting under an exception request will adhere to any additional security related procedures recommended by the technical and business staff of School of Communication and Information Dean's office.
Should an individual associated with the school but not employed at the school become responsible for NPPI, he or she must register as a data custodian. The responsibility of notice in this regard will fall upon the area director or the principal investigator for grant related research. For centers this will be either the faculty director or the staff executive director.

Proactive Restricted Data Discovery Processes

IT Services will use scanning tools to proactively try to identify Restricted Data that resides on systems within the school to ensure that it is adequately protected. These scanning tools will be used on a regular basis and any restricted data that is discovered will result in communications with the owner of the data to ensure that the data should be stored in its current location, that it is adequately protected, and to ensure that the individual is properly registered as a data custodian. Similarly, the Business Office will periodically conduct in-person audits for hardcopy restricted data.

Secure Removal and Disposal of NPPI

Any system that houses NPPI requires special attention prior to its disposal. Specifically, NPPI will need to be securely removed so that there are no traces of that data left on the existing system or device. When such a device needs to be disposed of, IT Services should be contacted to provide assistance with securely deleting such information through drive sanitization processes. This includes computers, copiers, fax machines, and portable storage devices.

Sensitive information in hardcopy form should be destroyed once it is no longer deemed necessary by school-wide and university-wide records retention policies. Hardcopy sensitive information should be cross shredded prior to disposal. Unnecessary NPPI should remain in a locked filing cabinet or desk until it is shredded. In addition, any credit card information recorded for the purposes of processing a transaction should be destroyed immediately after completing the transaction.

Security Training

All members of the School of Communication and Information are encouraged to complete an online information security awareness training session and take a quiz associated with that training. These training guidelines are also applicable to any registered data custodian whether he or she is part of the school or not.

RUTGERS
THE STATE UNIVERSITY
OF NEW JERSEY

Request to Telecommute

updated 2-16-15

Name: ____

Title: ____

Department: ____

1. I request to telecommute on the following basis:

   □ Regular

   Requested telecommuting days are:

   □ Monday □ Tuesday □ Wednesday □ Thursday □ Friday

   Requested telecommuting hours are:

   M:__________ T:__________ W:__________ Th:__________ F:__________

   □ Occasional

   I will provide __________ business days' notice when telecommuting is anticipated.

   □ Emergency

2. I request to begin telecommuting on: ______________ and continue until: ______________.

3. I intend to telecommute from (specify location and address):

   ____

   ____

4. I will require the following equipment / supplies:

   ____

   ____

5. I will perform the following duties and assignments:

   ____

   ____

Request to Telecommute (continued…)

I have read and understand the Telecommuting Policy and I agree to the duties, obligations, responsibilities and conditions described in the Policy.

I understand and agree that effective communication and satisfactory completion of stated duties and assignments are keys to successful telecommuting. I further agree that, among other things, I am responsible for furnishing and maintaining my remote worksite in a safe and professional manner; employing appropriate information protection and security measures; and complying with all other policies and guidelines of the University. I agree to provide access to my work site upon reasonable notice by any agent of the University to conduct inspections as may be deemed necessary.

I agree not to use any University equipment for private purposes, and not to allow family members or friends to access that equipment. I understand that the University may pursue recovery for any University property that is deliberately or negligently damaged or destroyed while in my custody. I shall promptly return all University equipment and data when requested by my supervisor, and agree to follow all software licensing provisions agreed to by the University. I certify that equipment utilized for telecommuting meets the University's telecommuting security standards. I understand that University data that resides on my workstation is owned by the University and subject to existing laws and policies governing the University.

I agree to notify my supervisor promptly when I am unable to perform work assignments due to equipment failure, illness, or other circumstances. I agree that no business meetings will be held in the alternate work location without specific approval of my supervisor. I agree that travel between the Alternate Work Location and the regular Work Location shall not be reimbursed. I also agree that telecommuting is not a substitute for child or dependent care and that other arrangements are necessary for care of dependents that are present in the Alternate Work Location.

I understand that telecommuting is a privilege that requires the approval of my department, which may be withdrawn or modified at such time as the department deems appropriate, and that any modifications to this arrangement must be set forth in writing. I also understand that except when established for emergency situations, I may end the telecommuting arrangement upon written notice to my supervisor.

____
Employee Signature

____
Date

TO COMPLETE THIS FORM, DOWNLOAD THE .DOC VERSION

RUTGERS
University Human Resources

Feasibility Assessment
Telecommuting Policy

This document is used to help the supervisor determine the feasibility of a particular position and/or employee to be engaged in a telecommuting agreement. The document will also assess the employee's and supervisor's work styles and determine if the styles would support a telecommuting arrangement.

Name of Telecommuter: ______________________________

Position Title: ______________________________

Name of Supervisor: ______________________________

Department/Unit: ______________________________

Job Assignments and Duties

The position must be classified as "NL" (not subject to overtime) Managerial, Professional, Supervisory or Confidential position.

List the key duties and percentage of time allocated to each duty.

1. ______________________________ % __________
2. ______________________________ % __________
3. ______________________________ % __________
4. ______________________________ % __________
5. ______________________________ % __________

Employee Assessment

This section will help you determine if the position's key duties lend themselves to telecommuting.

Do key duties require ongoing access to equipment, materials, and files that can only be accessed on Rutgers property? ❑ Yes ❑ No

Do key duties require extensive face-to-face contact with supervisors, other employees, clients, or the public on Rutgers property? ❑ Yes ❑ No

Do key duties require extensive time in meetings or performing work on Rutgers property? ❑ Yes ❑ No

Do security issues require key duties to be conducted on Rutgers property? ❑ Yes ❑ No

If you answered 'Ye's to any of the above questions, telecommuting might not be appropriate.

How reliant is this position on computer technology to accomplish key duties? ______________________________

____

What percentage of time is required on Rutgers property? % __________

The following tasks are typical of employees who telecommute. Indicate the percentage of time spent on appropriate tasks each week for the specified position.

Writing/editing	% _____ each week	Research	% _____ each week
Word processing	% _____ each week	Phone calls	% _____ each week
Data analysis	% _____ each week	Programming	% _____ each week
Administrative	% _____ each week	Email	% _____ each week
Reading	% _____ each week	Travel/visits	% _____ each week
Planning	% _____ each week	Other________	% _____ each week

Can the time spent on the above type of tasks support telecommuting? □ Yes □ No

If not, can you rearrange the position's duties (performed on the same day) to support telecommuting? □ Yes □ No

How frequently would you want the employee to telecommute?

□ One day per week □ Two days per week □ Three days per week

□ Once every two weeks □ Occasionally/special project □ Other: ______________________________

Do you need to add additional duties to support telecommuting? □ Yes □ No

Employee Assessment

This section will help you determine if the employee can work in a self-directed manner in managing his or her work and time.

Does the employee have a complete understanding of his or her job and performance expectations? □ Yes □ No

Does the employee regularly demonstrate that his or her approach to work is organized and dependable? □ Yes □ No

Is the employee highly productive? □ Yes □ No

Does the employee regularly meet deadlines? □ Yes □ No

Can the employee work independently and without constant supervision? □ Yes □ No

Can direction be provided by the phone? □ Yes □ No

Does the employee need/desire to be around coworkers? □ Yes □ No

Are there any known potential distractions at home (e.g., interruptions due to dependent care)? □ Yes □ No

Can the employee work in an environment with little structure? □ Yes □ No

Does the employee have the technology, including computer, appropriate software, and remote access capability, to work from home? □ Yes □ No

Does the employee have a suitable workspace at home? □ Yes □ No

Can the employee's performance at home be measured? □ Yes □ No

Based on the above, does the collective weight of Yes answers support the employee being a teleworker? □ Yes □ No

Supervisory Assessment

This section will help you determine if your managerial/supervisory style supports telecommuting.

Are your comfortable allowing employees to work largely autonomously? □ Yes □ No

Do you provide solutions when requested for assistance? □ Yes □ No

How frequently do you monitor the employee's work performance?

□ Daily □ Weekly □ Other Intervals

Are you comfortable communicating via email or telephone, as opposed to face-to-face? □ Yes □ No

Are you able to establish clear objectives? □ Yes □ No

Can you accurately measure the employee's performance and outcomes? □ Yes □ No

Can you accurately measure the employee's time worked? □ Yes □ No

Do you have a backup to monitor work in your absence (short and long term) □ Yes □ No

Do you trust that the employee will be productive notwithstanding lack of direct supervision? □ Yes □ No

Based on the above, does the collective weight of 'Yes' answers support the employee being a teleworker?? □ Yes □ No

Decision

Summarize your answers from the above assessment sections.

The position's key duties support telecommuting. □ Yes □ No

The employee meets the criteria to be a telecommuter. □ Yes □ No

My management/supervision style supports telecommuting. □ Yes □ No

My department supports telecommuting. □ Yes □ No

I should approve my employee's request to telecommute. □ Yes □ No

Proposed work schedule:

Comments:

RUTGERS
THE STATE UNIVERSITY
OF NEW JERSEY

University Telecommuting Agreement

updated 2-16-15

This is an agreement between____ ("Employee") and

____ ("Department") to establish the parameters of a

telecommuting agreement.

1. Telecommuting is established on the following basis:

   □ Regular

   The established telecommuting days are:

   □ Monday   □ Tuesday   □ Wednesday   □ Thursday   □ Friday

   The established telecommuting hours are:

   M:_____________ T:______________ W:_____________ Th:_____________ F:______________

   □ Occasional

   Employee will provide ______________ business days' notice when telecommuting will be performed.

   □ Emergency

2. This telecommuting arrangement will begin on: ________________ and continue until: ________________, or until ended by written notice by either the Employee or the Department.

3. The alternative work site address is:____

4. The Department will furnish the following equipment / supplies, and they will be returned to the Department within ______________ business days of the conclusion of this Agreement:

   ____

   ____

5. The duties and assignments that are authorized to be performed at the alternate worksite are:

   ____

   ____

6. The following methods and frequency of communication are agreed to:

   ____

   ____

7. Other relevant details not covered specifically in this Agreement:

   ____

   ____

University Telecommuting Agreement (continued…)

This is not a contract of employment between Rutgers University ("university") and the Employee and this does not provide any express or inherent rights to continued employment. This Agreement does not alter or supersede the terms of the existing employment relationship.

I have read and understand the Telecommuting Policy and I agree to the duties, obligations, responsibilities and conditions described in the Policy.

I understand and agree that effective communication and satisfactory completion of stated duties and assignments are keys to successful telecommuting. I further agree that, among other things, I am responsible for furnishing and maintaining my remote worksite in a safe and professional manner; employing appropriate information protection and security measures; and complying with all other policies and guidelines of the university. I agree to provide access to my work site upon reasonable notice by any agent of the university to conduct inspections as may be deemed necessary.

I agree not to use any university equipment for private purposes, and not to allow family members or friends to access that equipment. I understand that the university may pursue recovery for any University property that is deliberately or negligently damaged or destroyed while in my custody. I shall promptly return all university equipment and data when requested by my supervisor, and agree to follow all software licensing provisions agreed to by the university. I certify that equipment utilized for telecommuting meets the university's telecommuting security standards. I understand that university data that resides on my workstation is owned by the university and subject to existing laws and policies governing the university.

I agree to notify my supervisor promptly when I am unable to perform work assignments due to equipment failure, illness, or other circumstances. I agree that no business meetings will be held in the remote work location without specific approval of my supervisor. I agree that travel between the Alternate Work Location and the regular Work Location shall not be reimbursed. I also agree that telecommuting is not a substitute for child or dependent care and that other arrangements are necessary for care of dependents that are present in the Alternate Work Location.

I understand that telecommuting is a privilege that requires the approval of my department, which may be withdrawn or modified at such time as the department deems appropriate, and that any modifications to this arrangement must be set forth in writing. I also understand that except when established for emergency situations, I may end this telecommuting arrangement upon written notice to my supervisor.

	FOR THE UNIVERSITY:
______________________________	______________________________
Employee Signature	*Approver Signature*
______________________________	______________________________
Date	*Date*