THE UNIVERSITY OF RHODE ISLAND

PROCEDURES for Policy on Remote Work

Effective Date: June 20, 2022

Policy # 02.116.2

Introduction

The University of Rhode Island's Policy on Remote Work requires that non-faculty employees complete a Remote Work Agreement and abide by certain terms and conditions noted in the policy in order to undertake Remote Work for the University. These procedures, as amended from time to time, have been established to ensure compliance with the above policy.

Questions regarding these procedures should be directed to the Assistant Vice President for Human Resources at the University.

Procedure

In order to undertake Remote Work at the University of Rhode Island, an employee must make arrangements with their supervisor and receive approval from their Unit Manager (for the purposes of this policy, a Unit Manager an Academic Dean in any of the colleges, or if outside of the colleges, a direct report to a member of the President's Leadership Council) and the Office of Human Resources. The arrangement is memorialized in a Remote Work Agreement.

1. Employee must discuss options with supervisor or Unit Manager.
2. Employee will complete Remote Work Agreement.
3. If the Remote Work Agreement is acceptable to the Unit Manager, the employee and Unit Manager sign the Agreement.
4. Unit Manager must forward to the Office of Human Resources, Attn: AVP Human Resources.
5. If the Remote Work location is outside of Rhode Island, the AVP Human Resources must forward the Agreement to the Vice President for Administration and Finance for additional review and signature.
6. The Remote Work Agreement is filed with the Office of Human Resources.

Review and Renewal

The Remote Work arrangement is not automatically renewed but must be reviewed at the request of the employee. A new Remote Work Agreement must be completed per the above procedures and filed with the Office of Human Resources.

Using Personal Equipment for Remote Work

When possible, all Remote Work should be undertaken using University-owned Equipment. When an employee must use a personally-owned device to undertake Remote Work, that device must meet the same IT security requirements as University-owned devices. Employees with Remote Work arrangements who use personally-owned devices to conduct University business agree to the installation and maintenance of any device monitoring, device maintenance, security, or similar software, as well as appropriate patches and updates, to ensure that the personally-owned device is equal to any University-owned device in terms of IT security and endpoint protection.

THE
UNIVERSITY
OF RHODE ISLAND

Securing Your Personal Equipment

Use a separate login account

If other members of your household use the same computer, create a separate login account for your URI work and data, with a strong password that only you know. Using a separate login ensures other users on your computer cannot view or access your URI documents.

Encrypt all confidential data

If you have confidential University data on a computer that is located at home, or that comes home with you, that data must be encrypted. Check with your department's IT support staff to find out what encryption solutions are used in your department.

Back up your data

Data stored on your devices can be lost, accidentally deleted, or maliciously attacked. Protect your important files, data, and research by making electronic copies and storing them safely. Have multiple backup plans in place to fully secure your work as appropriate for the sensitivity of the data (e.g., cloud storage, encrypted flash drive, external hard drive). If you have a copy of your data and your device falls victim to ransomware or other cyber threats, you can restore the data from a backup.

Connect to campus with the Virtual Private Network

Connecting to URI's network from home increases the risk of data exposure or password compromise because you have to use networks that are not controlled by URI. To minimize these risks, **you must use the campus Virtual Private Network (VPN) when accessing URI resources.** Using a VPN will ensure that everything you do is encrypted as it goes over the network. VPN protects your data from electronic eavesdropping and is required to connect to some department and central resources from off campus. To find out how to install and use, see URI's VPN Enrollment Instructions.

Secure your home wireless network

Home wireless networks are easy to set up and extremely convenient to use. However, an insecure wireless environment poses several risks that need to be addressed:

- Anyone near your home can use your Internet connection.
- Anyone near your home may be able to access your computer.
- Anything sent over the wireless connection could be stolen.

The manuals that came with your wireless router should provide detailed information on how to secure your home wireless network. If you no longer have the manual, use the brand name and model type to search for an electronic copy online.

Keep your computer secure

If you are working on a computer that is not URI-owned, make sure that your operating system and applications are updated regularly. In addition, activate your computer's firewall protection and antivirus software. If you are working on university business on a computer at home, whether you or URI own the computer, you **must** take measures to secure your computer and mobile device**s. If you have both a URI owned device and a personal device only the URI owned device should be used for University business.**

NOTE: As outlined in the University Endpoint Protection Policy, Faculty and staff should avoid the use of personal laptops and desktops for conducting University business, including all administrative tasks, grading of student work, and sponsored research activities. When such use is necessary and involves accessing sensitive or Confidential University Data or interacting with University-owned systems using elevated privilege levels (such as User installation, patching or updating, large-scale data uploads or downloads, and similar) the following additional provisions shall apply:

- University-provided device monitoring, device management, and security software **must** be installed on the device.
- URI Virtual Private Network (VPN) service with multifactor authentication **must** be used.
- The device **must** utilize unique user identities with strong password or biometric identity verification in place.

Exceptions

None

THE
UNIVERSITY
OF RHODE ISLAND

Instructions: This is a digital form to be completed using *Adobe* software. You will need to create a digital signature in Adobe Acrobat for use with this form. Open this form in Adobe Acrobat, fill it out, and affix your digital signature. It must be filled out completely, including the identification of all URI-issued or personally-owned IT devices to be used for remote work. Contact the URI Chief Information Security Officer (security@uri.edu; 401-874-4787) for questions regarding IT security compliance for personally-owned devices. Remote access to University networks must be undertaken via a VPN. This form must have all your information, all computer information, your digital signature, your department manager's digital signature, and Human Resources digital approval before it goes to the Vice President for approval. Do not print, scan, or photocopy during the approval process.

Remote Work Agreement

Employee Information

Name: _____

Title: _____

Department: _____

Employee ID: _____

Email: _____

Contact Information

Cell Phone: _____

Alternative: _____

Remote Work Location: _____

Remote Work Schedule: Start Date: _____ End Date: _____ **(maximum 6 mos.)**

Please identify the days and times designated for remote work

(*All overtime must be approved in advance)

Day	*Work Hours (HH:MM - HH:MM)
Sunday	
Monday	
Tuesday	
Wednesday	
Thursday	
Friday	
Saturday	

THE
UNIVERSITY
OF RHODE ISLAND

University-Owned Equipment

Equipment Description (Make, Model)	URI Property Number and/or Serial Number

Software

The employee agrees to have access to the following software/applications housed on University servers. Access to University networks must be undertaken via a VPN.

Application	Note

Personal Equipment (Must meet current IT security standards)

Equipment Description	Notes

Special Circumstances, Terms and Conditions

THE
UNIVERSITY
OF RHODE ISLAND

AGREEMENT AND SIGNATURES:

This agreement must be signed by the employee, the employee's unit manager (for the purposes of this policy, an Academic Dean in any of the colleges, or if outside of the colleges, a direct report to a member of the Senior Leadership Team) and the Assistant Vice President for Human Resources (or their designee). In addition, should the remote work location be outside of Rhode Island, this agreement must also be signed by the Vice President for Administration and Finance (or their designee).

I, _____, attest that I have read the University of Rhode Island's Remote Work Arrangements policy and I agree to comply with the terms and conditions of this policy. I understand that my work responsibilities and expected levels of productivity will remain the same as if I were working at a University location.

1. I agree to maintain a safe work environment conducive to work productivity and be electronically accessible during work hours.
2. I agree to ensure arrangements, if applicable, for dependent care during work hours and agree to keep non-business disruptions (phone calls, visitors, etc.) to a minimum.
3. I agree to maintain standard work hours as noted in the Schedule above and will maintain appropriate work breaks. All overtime must be approved in advance.
4. I understand that I must seek approval for the discharge of vacation or other leave in the same manner as if I was working at a University location.
5. I understand that this agreement does not relieve me from attendance at meetings, trainings, or other mandatory on-site events within my department, barring any stipulations notes above.
6. I agree that I shall report any injury, equipment theft, loss, or damage immediately upon occurrence, allowing agents of the University to inspect my work location as applicable to the claim.
7. I agree that I shall work only on University-owned and configured equipment, unless noted otherwise under Personal Equipment (above) and I confirm all personally-owned devices meet the University's IT security compliance policies.
8. I agree that I shall maintain all endpoint security on any device used to access University networks. Additionally, I shall use a VPN connection for accessing any University network.
9. I shall return all University-owned equipment at once and in good condition upon termination of this agreement.
10. I understand that the University of Rhode Island or my supervisor may terminate this agreement at any time due to non-performance or, if due to a change in business operations, with four weeks' notice.
11. I understand that this agreement will not automatically renew but must be reviewed and resubmitted for renewal prior to the Remote Work End Date noted above.

_____
Employee Signature and Date

_____
Unit Manager/Supervisor Signature and Date

_____
Human Resources Administration Officer Signature and Date

_____
Vice President for Administration and Finance Signature and Date (Or Designee)