Approver Guide to Hard Stops, Risks, and Attestations in the Remote Work Agreement (RWA)

Here are key considerations for vetting Remote Work Agreements (RWAs) prior to School/College/Division (S/C/D) Approvers approving, denying, or pushing an RWA back for more/revised information.

Level 1 Approver: The Supervisor/Time Approver should verify the appropriateness of the RWA using the Remote Work Suitability Reference Guide, and confirm that the employee's answers reflect supervisor-employee discussions. If approved, the RWA is routed to Level 2 Approver (up through four possible levels, if established in a S/C/D).

Level 2, 3, 4 Approvers: These approvers (minimum Level 2; maximum Level 4) are appointed within each S/C/D. The *highest* approver in each S/C/D makes the final decision—and assumes risk. When there are risk flags, the highest approver should consult with corresponding consulting office(s), which advise on specific risks. See RISK CHART, pp. 3-6.

Consulting Offices: These include the Offices of Cybersecurity, Compliance, Export Control, Research and Sponsored Programs (RSP), and the Office of Human Resources (OHR) Payroll. These offices alert highest approvers to potential risks and make recommendations (i.e., they do not make decisions to approve or deny RWAs).

HARD STOPS: Conditions Inappropriate for Remote Work

Employees should **not** complete the Remote Work Agreement under these circumstances:

1. When seeking workplace flexibility (see definitions in Remote Work Policy).
    - **Why?** Because this agreement is strictly for remote work.
2. When an employee with a disability requests remote work as an accommodation.
    - **Why?** Because employees should contact their DDR for accommodations.
    - **Note:** Employees with disabilities can request remote work under the policy without making an accommodation request if they prefer to pursue an RWA without disclosing a disability. In this case, the RWA will be evaluated consistent with other RWAs , not as an accommodation under the Americans with Disabilities Act (ADA).
3. When attempting to work remotely from an international location without approval of "business necessity" from S/C/D Dean/Director/Vice Chancellor (VC). This is defined in the policy as a legitimate purpose that fulfills the mission and objectives of the university and is not solely for the personal benefit of an employee.
    - Examples of international RWAs that do *not* meet the definition of business necessity include (but are not limited to) vacation, personal illness, disability, family caregiving obligations, other personal reasons.
    - **Why?** Because approval of business necessity by S/C/D Dean/Director/VC is required per policy.
    - **Next Step:** The employee must obtain this approval *before* completing the agreement. The RWA requires that the employee document the reason for business necessity if approved. Employees seeking approval should discuss with their manager/department chair who can escalate to HR.
4. When attempting to work remotely from an E:1/E:2 embargoed country.
    - **Why?** Because in some cases, special licenses are required from the federal government, and licenses can take several months to obtain or may be denied altogether.
    - **Next Step:** The employee must email Export Control and Cybersecurity before completing an RWA.

(Continued next page)

5. When a foreign national working at UW–Madison is requesting to work off campus.
    - **Why?** Because immigration status may be affected in this scenario.
    - **Next Step:** The employee must contact their employing unit (local HR) and International Faculty and Staff Services (IFSS) before completing an RWA. HR and IFSS will assess and may involve the S/C/D's Dean's office.
        - All *non-student* employees on a UW-sponsored status (H-1B, TN, E-3, O-1, J-1) must contact IFSS before moving forward with an RWA. Immigration status may be affected by working remotely (even when from home). Those with other work authorizations should check with their sponsor (e.g., F-1s on OPT should talk to their international advisor, etc.). If the work authorization is based on a self-sponsored petition (e.g., asylum, DACA, H4), then IFSS does not need to be involved.
        - Regarding *student* employees on an F1 visa: As long as student employees are current students at UW–Madison on a valid I-20, no action is needed from an immigration perspective to work remotely from within the U.S., provided the employment is with UW– Madison. See on-campus job locations. (Because this employment is considered on-campus, there is not an impact on their visa.) If a student has departed the U.S., they have no U.S. immigration status.
    - **As of 07/12/23**: The U.S. Department of State, the federal agency responsible for managing the J-1 program, updated remote work authorization guidance for J-1 scholars. If you have foreign nationals currently working remotely more than 40%, they must create a new agreement *as soon as possible.* They must work on campus at least 60% to be compliant with updated immigration status regulations.

RISKS

There are eleven (11) risk flags that may be triggered by discrete answers on the RWA. Seven risk flags pertain to **international** requests. Of the remaining four risk flags, three involve use of **employee-owned hardware**** while working with Restricted data (including PHI) or Sensitive data. The remaining risk involves employees who work with PHI without using UW-approved data access/transfer/storage tools.

**Employee-owned hardware does *not* include *occasional* use of mobile devices, tablets, etc.

While the vast majority of RWAs from employees working remotely within Wisconsin and the U.S. are not flagged, highest approvers are strongly encouraged to vet any risk flags *prior* to approval of any RWA—by discussing risk(s) with the relevant consulting offices.

See chart beginning next page…

Risk	**The "Why"**	**Next Step(s)**
1. Business Necessity Approved? [**NO**]	This is required for International Remote Work Agreements, per policy. The S/C/D Dean, Director, or Vice Chancellor (or designee) must approve business necessity in order for the employee to be eligible to work remotely from an international location.	The employee must obtain this approval *before* completing an RWA. If business necessity has *not* been approved, they should discuss with their manager/ department chair who can escalate to HR. The employee will not be able to submit an RWA unless business necessity is indicated as approved and the reason is documented.
2. International Remote Work? [**YES**]	If an employee's remote work address is international, *regardless* of other information submitted in the RWA, the Offices of Compliance (Privacy) and Export Control must review information on the agreement to assess risk in their respective areas. For example, an employee's specific location and type of work needs to be reviewed by Export Control because licenses may need to be obtained from the federal government (and these can take several months to obtain or may be denied altogether). These offices will obtain more information and discuss risks with the highest approver. Additionally, while consultation with Risk Management is not necessary, it is important to note that significant insurance coverage issues may be identified.	The Office of Compliance (Privacy Officer) will review submitted information along with information available through other sources (such as ARROW) and will follow up with the employee when needed. Whenever Compliance is flagged, the highest approver will be alerted/advised about risks. Export Control will obtain more information (if necessary) by contacting appropriate parties and will contact all approvers to share its recommendations. Risk Management notification: • Highest approvers must understand that UW–Madison's Worker's Compensation (WC) coverage through the State of WI Self-Funded WC Program is *not* established to respond to occupational injuries/illnesses that occur for employees in the context of international RWAs. • Employees who work remotely outside of the U.S. and who are injured in the course of work are required to seek medical treatment *within Wisconsin* to receive coverage under UW-Madison's WC program. This is a notable risk for highest approvers to consider before evaluating the decision to approve international RWAs. Contact Risk Management with questions.

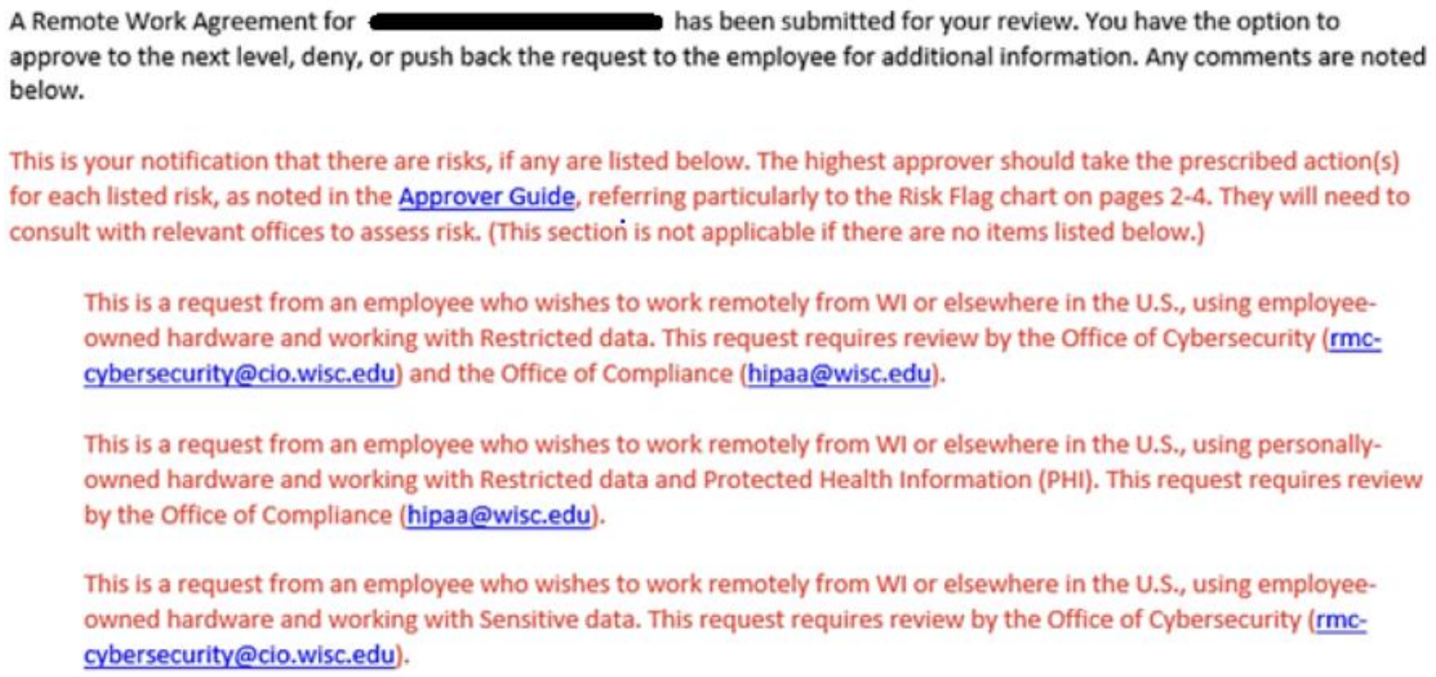
Chart continues next page…

Risk	The "Why"	Next Step(s)
3. Remote work from an International E1/E2 Embargoed Country? [**YES**]	All requests from employees who wish to work remotely from an E1/E2 embargoed international location must be reviewed by Export Control and Cybersecurity because of the high risk associated with these locations.	Highest approver *must* discuss risks with both **Export Control** and **Cybersecurity**. Licenses from the federal government are often required if the RWA is pursued, and may take several months to obtain or be denied altogether. (They are usually denied.) Both consulting offices will obtain more information directly from the employee, and: • Export Control will contact highest approver to share recommendations. • The Office of Cybersecurity will email the employee, manager and S/C/D HR contact to discuss the employee's level of risk. During these discussions, Cybersecurity may decide that the employee needs to enter additional information via OneTrust for generation of a risk report. This report should be reviewed and accepted by the highest approver *prior* to approving the RWA with these conditions.
4. International Remote Work with Sensitive Data, Using Employee-Owned Hardware? [**YES**]	There are high risks associated with this combination.	The Office of Cybersecurity will email the employee, manager and S/C/D HR contact to discuss the employee's level of risk. During these discussions, Cybersecurity may decide that the employee needs to enter additional information via OneTrust for generation of a risk report. This report should be reviewed and accepted by the highest approver *prior* to approving the RWA with these conditions.
5. International Remote Work with Restricted Data, Using Employee-Owned Hardware? [**YES**]	There are high risks associated with this combination, even if within the U.S. or WI. **The Office of Compliance does not recommend using employee-owned devices to access restricted data, including protected health information (PHI). Employee-owned devices used to access restricted data poses significant risks to the security of data both in transmission and storage. The Office of Compliance recommends using University owned or managed devices for accessing restricted data. S/C/D assumes additional risk associated with employee use of personal devices.	The Office of Compliance (Privacy Officer) will review submitted information along with information available through other sources (such as ARROW) and will follow up with the employee when needed. Whenever Compliance is flagged, the highest approver will be alerted/advised about risks. The Office of Cybersecurity will email the employee, manager and S/C/D HR contact to discuss the employee's level of risk. During these discussions, Cybersecurity may decide that the employee needs to enter additional information via OneTrust for generation of a risk report. This report should be reviewed and accepted by the highest approver *prior* to approving the RWA with these conditions.

Risk	The "Why"	Next Step(s)
6. Using Employee-Owned Hardware, with Sensitive Data? [**YES**]	There are high risks associated with this combination, even if within the U.S. or WI.	The Office of Cybersecurity will email the employee, manager and S/C/D HR contact to discuss the employee's level of risk. During these discussions, Cybersecurity may decide that the employee needs to enter additional information via OneTrust for generation of a risk report. This report should be reviewed and accepted by the highest approver *prior* to approving the RWA with these conditions.
7. Using Employee-Owned Hardware, with Restricted Data? [**YES**]	There are high risks associated with this combination, even if within the U.S. or WI. **The Office of Compliance does not recommend using employee-owned devices to access restricted data, including protected health information (PHI). Employee-owned devices used to access restricted data poses significant risks to the security of data both in transmission and storage. The Office of Compliance recommends using University owned or managed devices for accessing restricted data. S/C/D assumes additional risk associated with employee use of personal devices.	The Office of Compliance (Privacy Officer) will review submitted information along with information available through other sources (such as ARROW) and will follow up with the employee when needed. Whenever Compliance is flagged, the highest approver will be alerted/advised about risks. The Office of Cybersecurity will email the employee, manager and S/C/D HR contact to discuss the employee's level of risk. During these discussions, Cybersecurity may decide that the employee needs to enter additional information via OneTrust for generation of a risk report. This report should be reviewed and accepted by the highest approver *prior* to approving the RWA with these conditions.
8. Using Employee-Owned Hardware, with Sensitive Data, and Working with PHI? [**YES**]	There are high risks associated with this combination. **The Office of Compliance does not recommend using employee-owned devices to access restricted data, including protected health information (PHI). Employee-owned devices used to access restricted data poses significant risks to the security of data both in transmission and storage. The Office of Compliance recommends using University owned or managed devices for accessing restricted data. S/C/D assumes additional risk associated with employee use of personal devices.	The Office of Compliance (Privacy Officer) will review submitted information along with information available through other sources (such as ARROW) and will follow up with the employee when needed. Whenever Compliance is flagged, the highest approver will be alerted/advised about risks.

Risk	The "Why"	Next Step(s)
9. Working with PHI and not Limiting Access/Transfer/ Storage of Data to UW–Madison Approved Tools? [**YES**]	There are especially high risks associated with this combination.	The Office of Cybersecurity will email the employee, manager and S/C/D HR contact to discuss the employee's level of risk. During these discussions, Cybersecurity may decide that the employee needs to enter additional information via OneTrust for generation of a risk report. This report should be reviewed and accepted by the highest approver *prior* to approving the RWA with these conditions.
10. International Remote Work on Research Fund 133, 142,143, OR 144? [**YES**]	If the employee's work involves sponsored projects overseen by Research & Sponsored Programs (RSP), and the employee is planning to work remotely from an international location, the employee must discern (in conjunction with supervisor/PI/ department/division) whether they are paid on any of these funds: Fund 133, 143, or 144 (managed by RSP) or 142 (managed by CALS).	The PI/department is advised to email RSP as soon as possible with the Award ID/Project ID so RSP can review the terms and conditions of the award. (The PI/department/employee can access the award agreement with the sponsor via WISER on the Documents tab. This lists all terms, conditions, and sponsor regulations that the PI and UW–Madison must adhere to.) RSP will reach out to the highest-level approver at the division when they learn that international remote work on a sponsored project is being contemplated. RSP may need more information from the PI, department, or division. In some cases, the project sponsor may need to approve the employee's remote work, and obtaining this approval can take a month or more. If the award requires sponsor approval for international remote work, Research and Sponsored Programs (RSP) will work with the PI/department/division to prepare a request. RSP will contact the sponsor to request permission for employee to work remotely. In cases where sponsor approval is required, the division should ensure sponsor approval is obtained prior to approving remote work.
11. International Remote Work, and a Foreign National? [**YES**]	This poses a tax risk. If the employee is a foreign national, the employee is required to provide the Office of Human Resources Payroll Office documentation to ensure that the employee is appropriately taxed when working outside the U.S., and that they receive the correct tax reporting documents at year end. See the Foreign Source Income website.	No action needed by highest-level approver. This is informational only: The Office of Human Resources Payroll Office will work with the employee to collect the required foreign source income documentation. This alone need not delay approval of the agreement but is a required follow-up for OHR Payroll and the employee.

When a risk flag is triggered, the system will send the approver an email with specific information. Here's a sample:



A Remote Work Agreement for [redacted] has been submitted for your review. You have the option to approve to the next level, deny, or push back the request to the employee for additional information. Any comments are noted below.

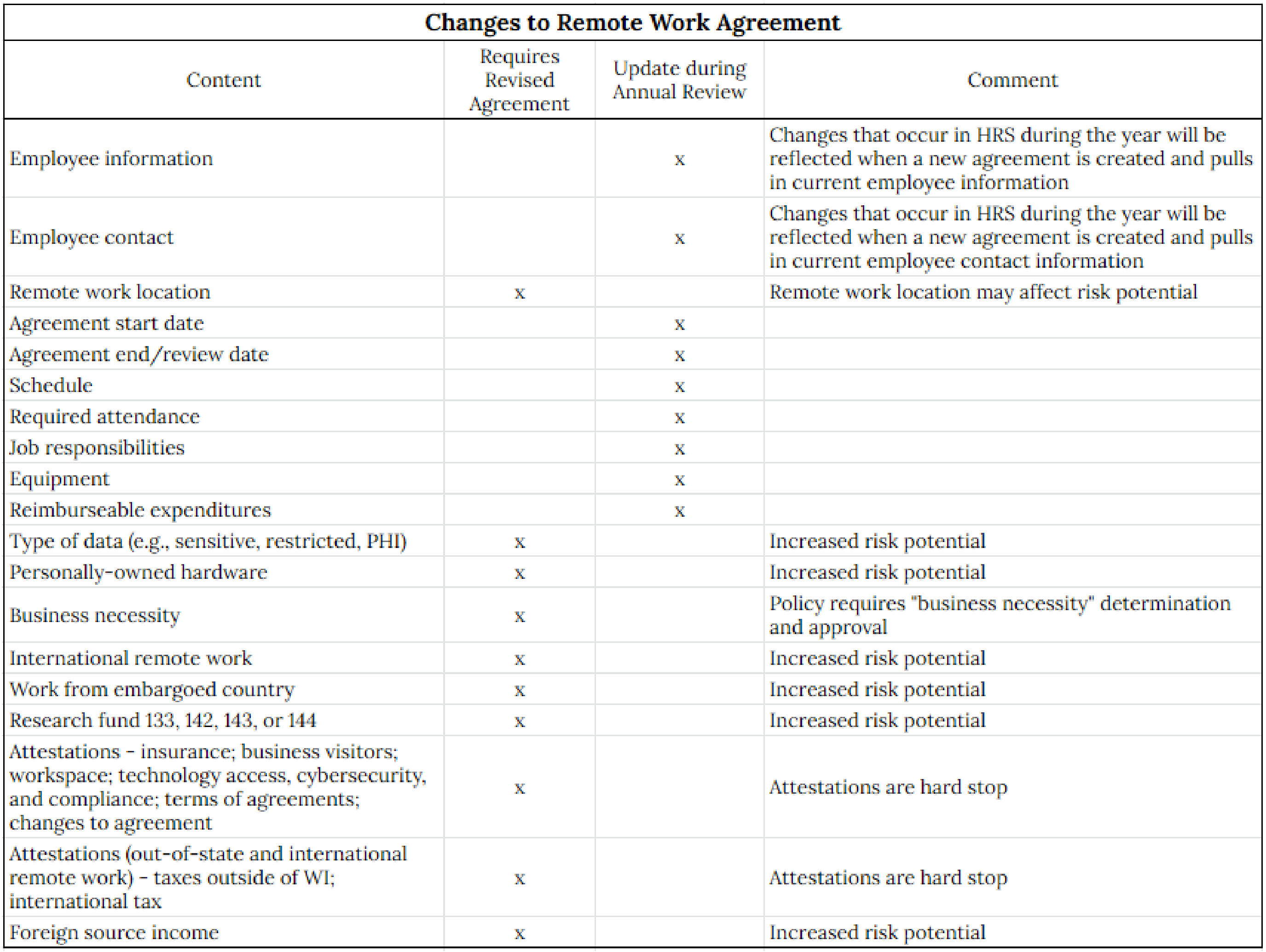
This is your notification that there are risks, if any are listed below. The highest approver should take the prescribed action(s) for each listed risk, as noted in the Approver Guide, referring particularly to the Risk Flag chart on pages 2-4. They will need to consult with relevant offices to assess risk. (This section is not applicable if there are no items listed below.)

> This is a request from an employee who wishes to work remotely from WI or elsewhere in the U.S., using employee-owned hardware and working with Restricted data. This request requires review by the Office of Cybersecurity (rmc-cybersecurity@cio.wisc.edu) and the Office of Compliance (hipaa@wisc.edu).
>
> This is a request from an employee who wishes to work remotely from WI or elsewhere in the U.S., using personally-owned hardware and working with Restricted data and Protected Health Information (PHI). This request requires review by the Office of Compliance (hipaa@wisc.edu).
>
> This is a request from an employee who wishes to work remotely from WI or elsewhere in the U.S., using employee-owned hardware and working with Sensitive data. This request requires review by the Office of Cybersecurity (rmc-cybersecurity@cio.wisc.edu).

Employees who have been working under an RWA that will soon expire must initiate a *new* RWA to cover the next reporting period.

(Continued next page)

Changes to an Approved RWA Requiring Submission of New RWA



Changes to Remote Work Agreement			
Content	Requires Revised Agreement	Update during Annual Review	Comment
Employee information		x	Changes that occur in HRS during the year will be reflected when a new agreement is created and pulls in current employee information
Employee contact		x	Changes that occur in HRS during the year will be reflected when a new agreement is created and pulls in current employee contact information
Remote work location	x		Remote work location may affect risk potential
Agreement start date		x	
Agreement end/review date		x	
Schedule		x	
Required attendance		x	
Job responsibilities		x	
Equipment		x	
Reimburseable expenditures		x	
Type of data (e.g., sensitive, restricted, PHI)	x		Increased risk potential
Personally-owned hardware	x		Increased risk potential
Business necessity	x		Policy requires "business necessity" determination and approval
International remote work	x		Increased risk potential
Work from embargoed country	x		Increased risk potential
Research fund 133, 142, 143, or 144	x		Increased risk potential
Attestations - insurance; business visitors; workspace; technology access, cybersecurity, and compliance; terms of agreements; changes to agreement	x		Attestations are hard stop
Attestations (out-of-state and international remote work) - taxes outside of WI; international tax	x		Attestations are hard stop
Foreign source income	x		Increased risk potential

Regarding changes to **Schedule** as listed in the chart above: schedule can be interpreted in two ways:

- changing the *days* onsite vs. remote (e.g., shifting remote work days from Mondays to Wednesdays)
- changing the *proportion* of onsite vs. remote work (e.g., shifting from 70%/20% to 20%/80%)

In either case, a supervisor or unit may wish to see this change reflected in an up-to-date RWA. While the policy does not require a new RWA in the event of change to Schedule, supervisors may require employees to submit an updated RWA. If this is the case, it is the responsibility of supervisors to communicate that to their employees.

(Continued next page)

ATTESTATIONS—for All Employees

There are eight (8) attestations for all employees, regardless of remote work location. The employee must acknowledge/ agree with all attestations in order to submit the agreement.

1. **INSURANCE**
   - *I understand that I am responsible for all instances of loss or damage that may occur to my employee-owned property and/or equipment. I also understand that I may be liable for damages or injury to third parties that occur at my remote work home location. I acknowledge that UW–Madison recommends I maintain personal homeowner's/condo/ renter's insurance to provide protection to myself against these personal risks.*
   - **Why?** Because this insurance protects employees, and not all employees may know this.
2. **BUSINESS VISITORS**
   - *I agree that I may not host business visitors, including students and other employees, in my home while engaged in remote work. I understand that hosting business visitors in my remote work location could result in personal legal liability to me.*
   - **Why?** Because if a business visitor (including colleagues or students) is injured while at an employee's home during the course of remote work, the employee may be personally liable for damages or injury to business visitors.
3. **WORKSPACE**
   - *I attest that my remote workspace is safe and functional and that I agree to:*
     - ***i.*** *Set up my workspace per the Workspace Checklist and as needed, use the resource, Ergonomics: A Guide to Setting Up Your Computer Workstation, to make any recommended modifications.*
     - ***ii.*** *Ensure smoke and fire detectors are installed and operating.*
     - ***iii.*** *Make certain my remote workspace is free from recognized fall hazards.*
     - ***iv.*** *Have a plan for seeking shelter during weather emergencies.*
   - **Why?** Because the university has a vested interested in maintaining the health and well-being of its employees and to avoid unnecessary worker's compensation claims due to avoidable work-related injury while employee is working remotely.
4. **TECHNOLOGY ACCESS, CYBERSECURITY, AND COMPLIANCE (1/3)**
   - *I agree to comply with UW–Madison's Division of Information Technology (DoIT) guidelines for securing a remote workstation; to maintain a safe and secure work environment at all times in compliance with UW–Madison's Office of Cybersecurity and Office of Compliance policies applicable to my work; to implement good information security practices in the home-office or alternative work site setting and will check with my supervisor when cybersecurity matters arise.*
   - **Why?** Because maintaining a secure remote workstation, work environment, and good security practices are essential protections for employees and UW–Madison.
5. **TECHNOLOGY ACCESS, CYBERSECURITY, AND COMPLIANCE (2/3)**
   - *I agree to take all necessary precautions to secure all university equipment and to protect the privacy, security, confidentiality, and integrity of data, files and other materials handled by me in the course of my work. This includes use of VPN, anti-virus, MFA DUO, Net ID login, etc.*
   - **Why?** Because protecting privacy and security via use of these tools are essential for protections for employees, students, research subjects, patients, and UW–Madison.
6. **TECHNOLOGY ACCESS, CYBERSECURITY, AND COMPLIANCE (3/3)**
   - *I agree to report the loss of any personal device that I am using in the course of my remote work, per UW–Madison's Incident Reporting and Response Policy.*

- **Why?** Because unauthorized access to restricted data and sensitive data can be detrimental to the affected individuals or the institution. UW–Madison has an obligation to mitigate associated risks, including conducting any required investigations.

7. **TERMS OF AGREEMENT**
    - *I have read and understand the above/attached expectations related to the remote work arrangement. I understand that my failure to adhere to these expectations and comply with UW–Madison's Remote Work Policy may result in the immediate termination of this remote work arrangement and/or discipline up to and including termination of employment.*
    - **Why?** Because employees who complete an RWA must adhere to the Remote Work Policy.
8. **CHANGES TO AGREEMENT**
    - *If anything in this agreement changes (e.g., work location, scope/type, access to different data types), I agree that I will complete a revised agreement.*
    - **Why?** Because changes may change the risk factors. When changes are made, risk needs to be re-evaluated. See Addendum: Changes to Agreement. See *Changes to Remote Work Agreement* above.

ATTESTATIONS—for U.S. (outside WI) Remote Employees

9. **TAXES OUTSIDE OF WI (FOR REMOTE WORK ELSEWHERE IN U.S.)**
    - *I understand that I must contact my division's HR/Payroll office regarding payroll tax outside the State of Wisconsin.*
    - **Why?** Employees working outside of Wisconsin will have tax implications. To avoid surprises, employees should work with their local payroll office.

ATTESTATIONS—for International (outside U.S.) Remote Employees

10. **INTERNATIONAL TAX (FOR INTERNATIONAL WORK)**
    - *I acknowledge that I am responsible for providing documents to my local HR to establish and verify my U.S. tax status and determine appropriate payroll taxation following the procedure documented here (insert hyperlink to OHR Payroll Instructions).*
    - **Why?** Employees working outside of the U.S. will have taxable foreign source income. To avoid tax implications, employees should work with OHR Payroll.

Other considerations:

Where is the agreement?

The Remote Work Agreement is located in HRS via employee self-service. The primary way employees access this information is in MyUW > **Personal Information** > **"Update my personal information."**

The timeout period for inactivity is 30 minutes, with a warning at 28 minutes. Employees can click save to continue completing the agreement at a later time. They can access their forms by name or form ID# following the instructions in the tip sheet: https://uwservice.wisconsin.edu/docs/publications/hr-employee-telework-agreement.pdf.

What else is on the agreement?

These sections apply to all employees who are requesting to work remotely:

1. **Employee Information & Contact** – When the employee logs on to MyUW and authenticates their ID using MFA DUO, this information is populated via HRS.
    - The employee with multiple jobs can select the correct job under "Working Title."
    - A separate Remote Work Agreement is required for each job when working remotely.
    - Supervisor and supervisor's email are included in contact information. If there is no supervisor listed in the "Reports To" field then the request will be assigned to the Time and Labor (TL) approver at the time the employee submits the agreement.
        i. If an employee has neither a supervisor nor time approver assigned, they will receive a message that they need to reach out to their supervisor to work with division HR to resolve this issue.
        ii. Either a Reports To (preferred) or a TL approver needs to be assigned in HRS before the employee can proceed.
2. **Remote Work Locations and Agreement Duration** – Here, the employee specifies:
    - **Remote work location(s)** – Addresses (including country) currently entered into HRS will populate here. When the employee chooses address type, the details of the address will populate based on what is listed in HRS.
    - **Up to three remote work address** – The employee can add up to three remote work addresses, by selecting "enter additional remote location."
        - **Home is defaulted for the employee.** The employee should use the drop-down menu to choose a different address. To update a home or mailing address, the employee will click the Update Addresses link.
        - If an employee needs to select an address that has not yet been entered into HRS, they will need to contact their local HR to add a new address into HRS. Once the new address is in HRS, it can be used in the Remote Work Agreement.
        - Note: RWAs require a physical location. RWA addresses cannot be mail service addresses (e.g., a PO Box, UPS box).
    - **Agreement Start Date** – Note: the start and actual date may differ, depending on the time to approve the agreement.
    - **Agreement End/Review Date** – The employee should work with supervisor who can check with HR about S/C/D-specific requirements related to RWA review periods. Approvers must review start/end dates and push back if employee has entered dates outside of the S/C/D approval window.
        - **Why?** Because the policy requires an annual review at minimum.
3. **Schedule –** The employee will record their schedule using either Daily Chart or General Hours. All schedules should be recorded using U.S. Central Standard Time (CST).
    - The employee selects **Daily Chart** to specify different work hours or remote work locations depending on the day of the week.
    - The employee selects **General Hours** if start and end times will be consistent from day to day and employee is working from only one remote location. The employee will enter on and off campus weekly average percentages of total time. (Percentages must be entered as integers and must total 100%, even if part time. These percentages represent "total effort.")
4. **Required Attendance** – This is a space for the employee to add situations for which onsite work is required. The employee is advised to discuss expectations with the supervisor, and to record these situations in the space provided.

- **Why?** Because sometimes onsite work may be required, even when the remote work schedule would suggest otherwise.

5. **Job Responsibilities –**
    - Employees who are seeking to work remotely *from an international location* must enter text or upload a PVL (if they have a copy).
        - i. **Why?** This is needed by various consulting offices who assess risk, for example, related to worker's compensation.
    - The employee must also answer: "Not including commuting to/from UW–Madison (or applicable onsite work location), will you use an automobile in the performance of your remote work duties/tasks?"
        - i. **Why?** Because *all* employees must be properly authorized by Risk Management to use an automobile when performing work responsibilities—whether onsite or remotely; whether within or outside of Wisconsin. Please reference How to Become an Authorized Driver.
6. **Equipment for Workspace** – Here, the employee will enter into open text boxes what they're using in the course of remote work, and answer one question. If a prompt does not apply, the employee must indicate N/A.
    - UW–Madison-Owned Hardware (e.g., computer equipment, external drives, instruments)
    - UW–Madison-Owned Communication Resources (e.g., mobile devices, tablets)
    - Office Equipment not including computer equipment provided to employee for remote work (e.g., office chairs, standing desks)
    - Employee-Owned Hardware, Communication Resources, and Office Equipment used in Remote Work (e.g., items that store/manipulate data such as computers and flash drives—but NOT routers/modems, monitors, nor personal mobile devices for *occasional* email use).
        - i. **Why?** Regular use of employee-owned hardware—particularly *computing* hardware which stores or manipulates data (e.g., include computers and flash drives; *not* routers/modems or monitors) can be risky in combination with other factors, such as the type of data that the employee works with. Please reference Protecting Data - Technical IT Staff and Approved Tools for Exchanging and/or Storing Protected Health Information (PHI).
        - ii. The Office of Compliance does not recommend using personal devices** to access restricted data, including protected health information (PHI). Use of personal devices for the access of restricted data poses significant risks to the security of the data both in transmission and storage. The Office of Compliance recommends using University owned or managed devices for accessing restricted data. Your school/college/division will assume the additional risk associated with employee use of personal devices.
**This does not refer to *occasional* use of mobile devices, tablets, etc.
        - iii. For more information:
            1. UW-133 HIPAA Security - Remote Access to Protected Health Information
            2. UW-136 HIPAA Security - Workstation and Mobile Device Use and Security Configuration
    - Additional equipment, if applicable
    - Reimbursable expenditures.
        - i. **Why?** Expenses that are reimbursable should be negotiated up front prior to agreement. See the UW-3024 Expense Reimbursement Policy for more information.
    - Question: "Will UW need to ship anything to you in your remote work location?"
        - i. **Why?** Because shipping to other countries can create risks that Export Control, for example, would need to mitigate.

7. **Technology Access, Cybersecurity, and Compliance**
    - Employee must answer: "What type(s) of data do you work with? (check all that apply - see definitions and more information)." The employee is required to select at least one type of data among the choices: Public, Internal, Sensitive, and Restricted.
        i. **Why?** Because while working with public and internal data pose less risk, working with sensitive and restricted data from remote work locations can pose risk in combination with other factors, such as working remotely on employee-owned hardware, or working internationally.
        ii. If YES to Restricted Data, employee is asked:
            1. Are you working with Protected Health Information (PHI)? If YES, employee will see this message: "When PHI is involved, the Office of Compliance will review any prior instances of HIPAA-related concern."
            2. Can the goals of your work in a remote location be achieved by using de-identified data? If NO: have you completed current UW-Madison HIPAA Training?
                a. **Why?** Sometimes the employee can mitigate risk by working with deidentified data. HIPAA training is critical when this is not possible.
        iii. If YES to Restricted data and YES to PHI, employee is asked: Will you limit your access/transfer/storage of this data to UW approved tools?
            1. **Why?** Using non-UW approved tools creates compliance risks.
    - Employee must answer: The specific question is: Are you *regularly* using employee-owned hardware as your primary device when accessing/downloading/transferring data?
        i. **Why?** Using employee-owned hardware while working remotely, in concert with other factors, such as the type of data worked with, creates compliance risks. If the employee answers YES, the employee will see a statement directing them to be sure to document that hardware in the Equipment section.
        ii. The Office of Compliance does not recommend using personal devices** to access restricted data, including protected health information (PHI). Use of personal devices for the access of restricted data poses significant risks to the security of the data both in transmission and storage. The Office of Compliance recommends using University owned or managed devices for accessing restricted data. Your school/college/division will assume the additional risk associated with employee use of personal devices.
        **This does not refer to *occasional* use of mobile devices, tablets, etc.
        iii. For more information:
            1. UW-133 HIPAA Security - Remote Access to Protected Health Information
            2. UW-136 HIPAA Security - Workstation and Mobile Device Use and Security Configuration

This section applies only to employees who are requesting to work remotely out-of-state (within U.S.):

Payroll Tax – The employee will be asked to attest to the following statement:

- *I understand that I must contact my division's HR/Payroll office regarding payroll tax outside the State of Wisconsin.* **Why**? Employees working outside of Wisconsin will have tax implications. To avoid surprises, employees should work with their local payroll office.

This section applies only to employees who are requesting to work remotely internationally:

International Remote Work – The employee will be asked questions:

- **General questions** – The employee will be asked the following:
  1. Approved by S/C/D Dean, Director, or Vice Chancellor as Business Necessity? If the employee answers YES, the employee will be required to document the reason for business necessity. **Why?** Without approval of business necessity, the agreement itself may not be approved.
  2. Country of Citizenship (with up to two dropdowns for those with dual citizenship). **Why?** Because citizenship poses a greater risk in concert with other factors, such as location of work.
  3. Did you previously work for UW-Madison while living in the U.S.? **Why?** To assess the likelihood of UW–Madison being subject to the employment laws of the foreign jurisdiction.
  4. Do you plan to move to the U.S. while working for UW-Madison? **Why?** To assess the likelihood of UW–Madison being subject to the employment laws of the foreign jurisdiction.
- **Export Control** – The employee will be asked the following:
  1. Is an export license required for you to conduct this work internationally? To check before answering, read Export Control | Research (click on licenses). **Why?** Because if yes, Export Control will have to apply for a license from the federal government.
  2. Will your remote work be conducted from an U.S. government E:1/E:2 embargoed country Export ControlE:1/E:2 countries (scroll to bottom of the page)? **Why?** Because these agreements are usually denied. If the agreement is pursued, licenses from the federal government may be required, and may take several months to obtain, or be denied altogether.
  3. Does your job require that you access information that is Export Controlled under the International Trafficking in Arms Regulations (ITAR) or Export Administration Regulations (EAR)? **Why?** Because if yes, this poses greater risk. An export license from the federal government may be required.
  4. The employee is notified in the agreement that if they answer YES to any of the above, they must email the Offices of Export Control and Cybersecurity before completing the Remote Work Agreement.
- **Research and Sponsored Programs** – The employee will be asked: “Are you currently paid or will you be paid on sponsored projects, i.e., funds 133, 142,143, or 144?” **Why?** Because the project sponsor may have to approve remote work. See the Risk Chart, risk #10 above for more detail.
- **Foreign Source Income –** Please indicate if you are a foreign national working outside of the United States. **Why?** Because the Office of Human Resources Payroll Office will work with the employee to collect the required documentation. No action is needed on the part of highest approvers. This indicates required follow-up for OHR Payroll and employee.

(Continued next page)

What might our consulting offices look for behind the scenes?

Some consulting offices do not need to be consulted *prior to approval* but will work to mitigate risks on the back end.

For example:

- Risk Management will pull reports of approved agreements to assess insurance and liability risk for employees working remotely out-of-state (in the U.S.) and internationally.
    - **Why?** Risk Management will utilize these reports to evaluate and determine need to secure insurance coverage for out-of-state and international risks, in consultation with State of Wisconsin Department of Administration Bureau of State Risk Management, which provides insurance coverage for UW–Madison employees (as for employees of all state agencies) through the State of Wisconsin's self-funded insurance programs.
- The Office of Legal Affairs (OLA) will help arrange outside counsel if UW–Madison or its employees (for actions in the course/scope of employment) are sued in another state or country for something related to their work.
    - **Why?** The DOJ provides defense counsel if UW–Madison or employees (for actions in the course/scope of employment) are sued in Wisconsin, but this counsel is not available for employees who are sued in another state or country for something related to their work.
- The Office of Human Resources Payroll Office will respond to any wage verifications or employment verifications required by the state in which an employee is working remotely if the employee is laid off. The employee would follow standard unemployment procedures.

See additional resources:

- Remote Work: Guidance and Resources for Employees
- Remote Work: Guidance and Resources for Supervisors
- Remote Work Suitability Assessment for Managers (Note: Each school, college, or division (S/C/D) determines the specific procedures for evaluating and approving or denying a remote work request. This resource is intended as a general resource. The process outlined in this resource may differ based on the S/C/D.)

Last updated July 14, 2023