onetrust

1 Primary Contact Information

1.1 **Contact Name for the lead researcher/Primary Investigator for this project.**

Response

Not answered

1.2 **Contact Phone Number:**

Response

Not answered

1.3 **Contact Email Address:**

Response

Not answered

1.4 **What Division is responsible for the project?**

Providing your Division helps us understand who yourRisk Executive is. Risk Executives have the authority to accept the risk of operating the department/system on behalf of the institution. Risk Executives ensure that: (i) security risk-related considerations for individual information systems, to include the authorization decisions, are viewed from an organization-wide perspective concerning the overall strategic goals and objectives of the organization in carrying out its missions and business functions; and (ii) managing information system-related security risks is consistent across the organization, reflects organizational risk tolerance, and considers other risks affecting mission/business success.

Select your Division from the dropdown, or start typing to filter:

Response

Not answered

1.5 **What Department is responsible for the project?**

If your Department is not listed, please contact the Office of Cybersecurity OneTrust administrators at onetrustadmins@office365.wisc.edu to have it added.

Providing your Department helps us understand where potential compliance gaps exist. It also helps us compile a complete risk profile for each Department on campus to ensure that those who are high risk or need assistance are receiving adequate attention.

Select your Department from the dropdown, or start typing to filter:

Response

Not answered

1.6 **Who provides primary IT support for you or your department? (Individual or Group)**

Assessments typically result in improvement suggestions that would be made by IT on workstations, servers, or some other piece of infrastructure. It is helpful to know who can answer questions about items such as current workstation configuration and who would be making suggested changes for you.

Response

Not sure

1.7 **IT Support Email:**

Response

Not sure

2 Federally Funded Research Project Details

2.1 **What is the Federal Award number or ID of this project?**

Please provide the ID number for the federally funded award/project you are working on.

Response

Not answered

2.2 **What is the common name of this research project?**

Is there a common name for the project you are working on.

Response

Not answered

2.3 **Who is the lead PI/Researcher fo this project?**

Please include the full name of the lead Primary Investigator or Researcher for this research project.

Response

Not sure Not applicable

2.4 **Please list all the "covered individuals" you have working on this project by name and position.**

This entry represents the individuals who will be working on this research project, will have access to the research data and will be included in this attestation for compliance.

Definition of Covered Individual: A person who contributes in a substantive way to the scientific development or execution of a research and development (R&D) award carried out with support from a federal research agency AND is designated as a covered individual by the federal research agency concerned. Covered individuals include principal investigators/project directors, co-investigators, those listed as senior project personnel/key project personnel, postdoctoral researchers/associates, and graduate and undergraduate students.

If you have a list of the research project team members, this can be attached.

Response

Not answered

3 NSPM-33 Questions

3.1 **Do your covered individuals complete UW-Madison annual Cybersecurity Awareness Training?**

Criteria for Yes:

- *Can you provide documentation from Workday?*
- *Can you provide validation from the Office of Cybersecurity?*

Resources:
For questions on Cybersecurity Awareness Training: https://it.wisc.edu/about/division-of-information-technology/enterprise-information-security-services/office-of-cybersecurity/cybersecurity-awareness-training/

Response

Yes No

3.2 **Do you maintain a list of individuals who are allowed to access research data?**

Criteria for Yes:
Do you have a list of users who will have access to the research data for this project?

Resource:
This information could come from a Google Sheet, an excel spreadsheet, could be pulled from RAMP or any other local storage tool.

Please attach that list for validation.

Response

Yes No Partial

3.3 **Do you have a process to limit users/employees to only the information systems, roles, or applications they are permitted and that are needed for their jobs?**

Criteria for Yes:

- *Do you apply role-based access (write, read, etc.)*
- *Is there documentation that defines the different access that different "covered individuals" should have for your project?*

Resources:

Response

Yes No Partial

3.4 **When accessing research data, do you either use campus managed assets and/or, with non-campus/personal assets, do you use campus network or VPN services?**

Criteria for Yes:

- *Are you only using UW-Owned and/or UW-Managed devices to access your research data?*
- *If you are allowing personal devices to access this research data, are there technical controls in place to secure this access (examples below)?*
- *VPN*
- *Remote Desktop*
- *HIP Checks*
- *Are you utilizing UW-Madison storage systems to secure your research data (examples below)?*
- *Restricted Research Drive*
- *RedCap*
- *ELN*
- *Secure Box*

Resources:

- *Network diagram for project data management*
- *Documentation of how data is stored accessed or utilized by project team members.*

Response

Yes No Partial

3.5 **Does everyone posting your research data understand and validate that the information is acceptable for public consumption?**

Criteria for Yes:

- *Do you have a process to follow for verifying that research data has been approved to be posted publicly?*
- *If using WiscWeb or another campus central resource, are you reviewing your user list?*

Resources:

- *List of publicly available resources in use*
- *Steps to take for approval to make research data public*

Response

Yes No Partial

3.6 **Do you have a process to assign a unique identifier to each user, system process, and asset used to access or store research data?**

Criteria for Yes:

- *Does each user with access to the data have a unique NetId?*
- *Shared service accounts, where multiple people use the same account credentials, are**NOT** used to access data for this project.*
- *Is your unit enrolled in and using campus active directory services (CADS)?*

Resources:

- *Your local IT team can assist with responses to this question.*

Response

Yes No Partial

3.7 **Do you have a process to authenticate each user, system process, and asset before it can access research data?**

Criteria for Yes:

- *Do you use UW issued federated login (such as campus NetID) login on your devices that access research data?*
- *Are you limiting the use of personal device access (ie VPN, remote desktop, etc.)*

Resources:

- *Your local IT team can assist with responses to this question.*

Response

Yes No Partial

3.8 **Do you have a process to validate that campus firewall rules only allow appropriate access to your research data?**

Criteria for Yes:

- *Do you use the GlobalProtect VPN while off campus to access research data?*
- *Do you have a process to validate that campus firewall rules only allow appropriate access to research data?*
- *Are you able to document the process by which campus firewall rules are validated?*

Resources:

- *Check with your units IT team for VPN support.*

Response

Yes No Partial

3.9 **Does your group keep publicly accessible systems, such as websites, on a separate network from the rest of your research data assets?**

Criteria for Yes:
Have you completed external scans of the systems to verify security?

Resources:
Check with your units local IT team

Response

Yes No I don't know

3.10 **Do you have ransomware protection installed on assets that access and store research data?**

Criteria for Yes:

- *Do you have Cisco Secure installed on assets that access research data?*
- *Are the assets with Cisco Secure installed in a "Protect" policy?*

Resources:

- *Validation can occur through Cisco Secure Console*
- *Check with your units local IT team*

Response

Yes No Partial

3.11 **Do you have a process to identify and apply patches and updates for systems that access or store research data?**

Criteria for Yes:

- *Do you have an established process for software and hardware patching and updates?*
- *Do you have Qualys Cloud Agent installed on your assets that access or store research data?*
- *Do you have BigFix, Workspace One, or Automatic Operating System updates installed on the devices accessing this research data?*

Resources:

- *Endpoint Management campus Documentation: https://it.wisc.edu/services/endpoint-management/*
- *Check with your units local IT team*

Response

Yes No Partial

3.12 **Do you have malicious code protection installed on assets that access and store your research data?**

Criteria for Yes:

- *Do you have Cisco Secure installed on all endpoints?*
- *Are the assets with Cisco Secure installed in a "Protect" policy?*
- *Do you have malicious code protection installed on assets that access and store research data?*
- *Is UW-Madison providing Proofpoint services to your unit?*
- *Do you have Windows Defender installed?*

Resources:

- *Have you enabled anti-virus on the personally owned devices accessing your data?https://it.wisc.edu/services/antivirus-software/*
- *Have you validated your antivirus installation through Cisco Secure console*
- *Proofpoint Services: https://it.wisc.edu/news/changes-coming-soon-to-your-email-inbox/*
- *Check with your units local IT team*

Response

Yes No Partial

3.13 **Do you have a process for updating malicious code protection software when new versions are available?**

Criteria for Yes:

- *Does your IT team us Cisco Secure in 'Protect' mode?*
- *Do you have windows defender installed?*

Resource:
Your local IT team can assist with responses to this question.

Response

Yes No Partial

3.14 **Do you have a process for performing real-time and periodic scans of files using malicious code protection software?**

Criteria for Yes:

- *Do you have Cisco Secure installed on assets that access research data?*
- *Are the assets with Cisco Secure installed in a "Protect" policy?*
- *Do you have a process for performing real-time and periodic scans of files using malicious code protection software?*

Resources:
Check with your units local IT team

Response

Yes No Partial

3.15 **Do you routinely seek cybersecurity assessments for significant new or changed IT systems and procurements?**

Criteria for Yes:

- *When new tools or services are required, are you contacting the appropriate teams for assistance to ensure data security?*

Resources:

- *Office of Cybersecurity - RMC*
- *S/C/I/D IT support team inquiries regarding security*

Response

Yes No I don't know

4 CMMC Questions

4.1 **CMMC Level 1 Compliance Attestation**

*The Cybersecurity Maturity Model Certification (CMMC) will be required in 2026 by research projects which access and store Department of Defense data. Responding to these additional 5 questions **now** allows movement toward achieving Level 1 CMMC Self-Attestation should you need it.*

For more information: https://www.dcsa.mil/Industrial-Security/Controlled-Unclassified-Information-CUI/Cybersecurity-Maturity-Model-Certification-CMMC/

Response

Not answered

4.2 **Do you erase or destroy media containing research data prior to disposal or reuse?**

Criteria for Yes:
Do you erase or destroy media containing research data prior to disposal or reuse?

Resources:
Swap records if media is sent to SWAP for disposal.
Vendor certification of data removal if a third-party is utilized.

Response

Yes No I don't know

4.3 **Do you protect assets used in research so they cannot be physically accessed by unauthorized individuals?**

Criteria for Yes:

- *Does your unit have a policy that limits the movement of visitors in your research area?*
- *Do you have a screenlock timer turned on?*
- *Are you participating in MFA?*

Resources:

Response

Yes No Partial

4.4 **Do you escort visitors and monitor their activity in spaces where research data and assets are stored?**

Criteria for Yes:

- *Are there logs kept of visitors entering your research space?*
- *Is there a policy by your unit as to who can enter your physical research space?*
- *Do you escort visitors and monitor visitor activity in spaces where research data and assets are stored?*

Resources:

Response

Yes No I don't know

4.5 **Do you keep a record of visitors to areas where research data assets are stored?**

Criteria for Yes:
Do you keep a record of visitors to areas where research data assets are stored?

Resources:

Response

Yes No I don't know

4.6 **Do you utilize physical controls, such as keys or access cards, to access spaces where research data assets are stored?**

Criteria for Yes:
Provide any information about how the physical space is secured where your research project happens.

Resources:

Response

Yes No I don't know

onetrust

5 Thank You

5.1 Thank you

Thank you for completing this questionnaire to document your compliance with NSPM-33 Cybersecurity requirements.

Once your questionnaire is completed, this is what you can expect:

1. *The Office of Cybersecurity (RMC) will confirm completion via e-mail to the Lead PI*
2. *RMC will review the responses to the questionnaire and determine what security gaps may exist*
3. *RMC will generate a report that outlines these security gaps and offer options to improve/remove the gaps*
4. *RMC will deliver the final report to the Lead PI, the IT team and Leadership within Research and Sponsored Programs who are responsible for Research Compliance*

For any additional questions, please contact the Office of Cybersecurity - Risk Management & Compliance unit at rmc-cybersecurity@cio.wisc.edu

Response

Not answered