CUI Checklist

This checklist provides the generalized requirements for building and maintaining a CUI-compliant information system to store and manage data.

1. Identify and implement controls that limit access to the system and data strictly to individuals affiliated with the research project.
2. Ensure that researchers, administrators, and technologists are informed of the security risks associated with their activities and of methods required to reduce those risks.
3. Implement system audit controls to record and report events deemed unlawful, unauthorized, or inappropriate to the research project or to UW-Madison. Events should be associated with an individual user.
4. Document and maintain an inventory of the information system assets (e.g. servers, laptops, mobile devices, and software applications) and their security configuration settings.
5. Identify and maintain an inventory of researchers, administrators, and technologists who have access to the information systems being used to support the research project. Each user should have a unique account (e.g. NetID) for authenticating to applications, servers, workstations, laptops, and mobile devices.
6. Follow the UW-Madison Incident Reporting Policy and Procedure (https://kb.wisc.edu/itpolicy/cio-incident-reporting-policy) for reporting any potential compromises relating to the research data or the systems used to support the project.
7. Create and maintain processes for managing the lifecycle of the information systems used to support the research project. This includes applying patches to applications and servers as well as having a data and information disposal plan
8. Control physical access to and securely store media assets containing CUI by limiting access to CUI authorized users and sanitizing or destroying media containing CUI before disposal or reuse.
9. Conduct screening activities (e.g. background checks) when recruiting and on-boarding researchers, administrators, and technologists who will have access to CUI and ensure access is removed when a researcher, administrator or technologist is off-boarded from the research project.
10. Physical access to organizational information systems, equipment, and the respective operating environments should be strictly limited to authorized individuals. These spaces should be monitored.
11. Periodic risk assessments should be conducted to ensure security controls are working as designed.
12. The information system should be monitored to detect and report indicators of potential compromises, data exfiltration, or other misuse.