Guidance on Research Conducted Remotely

I. Intellectual Property

Any intellectual property (IP) arising from research conducted by students or faculty ("Researchers") in most cases is owned by USA. Other entities, such as third party licensees, IUCRC members, or those paying for sponsored research, may have current or potential IP rights to any invention arising from the research.

Students must sign confidentiality agreements when working on research that could give rise to intellectual property and particularly when the research is paid for by outside parties (private sector funding, IUCRC memberships, material transfer agreements, etc.).

Per University policy (found at this link) Laboratory Notebooks and research data are the property of the University of South Alabama. To ensure the security of data, Laboratory Notebooks will remain on campus at all times. Exceptions to this policy will only be allowed in situations where it is critical to security or research continuity. Requests for exceptions to this policy must be sent in writing to:

Dr. Andrew Byrd
Director of the Office of Commercialization and Industry Collaboration
251-460-7932
andrewbyrd@southalabama.edu

Dr. Byrd will review the request and he will approve when appropriate. The request must include the reason for removal to a remote location.

II. Personally-Owned Computers:

In general, personally-owned computers must not be used to conduct off-campus research without prior written authorization from the principal investigator, faculty advisor or project lead. At times research may have to be continued off-campus through remote means ("Remote Research") due to a declared campus partial or complete closure (e.g., hurricanes, tornados, pandemics, etc.) (collectively "Closures").

When Remote Research is necessary for continuity due to a Closure, the following guidance applies to research and communications about that research.

III. General Cybersecurity Guidance

It is USA policy for faculty and student researchers to use, at a minimum, that level of security for research that is required under the terms of the grant, contract or sponsorship agreement. Any exceptions can occur only if waived or modified by the sponsor. USA policy states that faculty and students will apply that level of security on a project that is commensurate with that which should be required given the damage that disclosure or theft might create (Collectively "General USA Cyber Policy"). This is regardless whether or not a sponsor specifies the level or types of security. In some cases, that could mean that Remote Research cannot be conducted.

Remote Research obviously offers greater opportunity for theft of data or hacking of data. When there is use of, or access to classified or confidential unclassified information (CUI), or protected health information (PHI), researchers must comply with those technical safeguards as directed by applicable statutes, regulations, directives, and guidance or contract requirements. Likewise, researchers must follow all requirements set forth in the grant, contract or sponsorship agreement. In the absence of any guidance in those agreements, then the General USA Cyber Policy shall apply. USA is developing a baseline of recommended security practices for University employees engaging in at-home work. Once finalized, these can be used in conjunction with other applicable policies or directives.

IV. Remote Research

Under normal circumstances, certain types of research may only be conducted on campus, in controlled environments, using USA computers and secure servers, with no USA data leaving campus in any form. During Closures, research may be conducted remotely so long as it is approved by the faculty advisor and ORED VP, and complies with any requirements of the grant, contract or sponsorship agreement (unless those latter provisions have been waived in writing). In the absence of any specific requirements, the General USA Cyber Policy shall apply.

During Closures, researchers will make every effort to work on elements of a project in such a manner that will not risk exposure of proprietary or otherwise confidential ideas. This is particularly true when the resulting damage caused by disclosure of information on sensitive elements is substantial and irreversible.

V. Proprietary Data

If you know or reasonably suspect that proprietary data, methods or conclusions (collectively "Proprietary Data") are involved, then the following technical safeguards shall be used if conducting Remote Research:

1. Execution of a confidentiality agreement by anyone not otherwise bound (approved student version found at this link);
2. Password protected access to any computer used;
3. Up to date malware and anti-virus software installed on the computer used;
4. Storage of Proprietary Data is restricted to USA approved servers and storage systems;
5. Encryption of any Proprietary Data that must be stored on the computer;
6. Encryption of communications, including settings on communications platforms like Zoom (see link);
7. Access via an approved USA VPN;
8. Use of a password protected network;
9. Use of passwords containing at least 8 digits (requiring numbers, letters and special characters);
10. Proprietary Data may not be downloaded to a thumb drive;
11. Proprietary Data may not be attached to an email and sent to another person;
12. Method to confirm that any Proprietary Data generated remotely is ultimately stored on the appropriate USA approved server or storage system;
13. Method to confirm that any Proprietary Data stored inadvertently or deliberately on personally-owned computers is transferred to the appropriate USA approved server or storage system;
14. Method to confirm that any Proprietary Data stored inadvertently or deliberately on personally-owned computers is permanently deleted; and
15. Written confirmation by the faculty advisor outlining implementation of the technical safeguards.

For further information or questions, contact:

Dr. Michael Chambers
Associate Vice President of Research
michaelchambers@southalabama.edu
251-460-6333

Chris Cannon
Assistant Vice President and Director
Information Technology Services
ccannon@southalabama.edu
251-460-6161