# Protecting Export-controlled information

When research conducted at the University involves export controlled information, certain protective measures must be put in place in order to adequately safeguard that information. At VCU, we use Technology Control Plans (TCP) to outline those controls. A TCP is a protocol that outlines the procedures to secure certain export-controlled items (technical data, materials, software, or hardware) from unauthorized use, access, and observation by non-U.S. persons. The **Export Control** staff, with assistance from the Principal Investigator (PI), will develop a TCP that is designed for the specific project. The PI is the ultimate responsible party for adherence to the TCP by project personnel.

Examples of security measures for protecting export-controlled information are (but not limited to):

● Authorized personnel working on the project must be clearly identified.

● Project data and/or materials must be physically shielded from observation by unauthorized individuals by operating in secured laboratory spaces, or during secure time blocks when observation by unauthorized persons is prevented.

● Export Controlled Information must be clearly identified and marked as export controlled.

● Both soft and hardcopy data, lab notebooks, reports, and research materials are stored in locked cabinets; preferably located in rooms with key-controlled access.

● Tangible items like equipment and associated operating manuals and schematic diagrams containing identified "export controlled" technology are to be physically secured from unauthorized access.

● Appropriate measures will be taken to secure controlled electronic information. Such measures may include: User ID, password control, SSL or other approved encryption technology. Database access may be managed via a Virtual Private Network (VPN). Only authorized users can access the site and all transmissions of data over the internet will be encrypted using 128-bit Secure Sockets Layer (SSL) or other advanced, federally approved encryption technology.

● Discussions about the project or work products are limited to the identified contributing investigators and are held only in areas where unauthorized personnel are not present. Discussions with third party sub-contractors are only to be conducted under signed agreements that fully respect the non-U.S. citizen limitations for such disclosures.

If you think you might be working with export controlled data or information, or have questions regarding the Technology Control Plan, please reach out to exportctrl@vcu.edu.