Stony Brook University

Security & Safety Bulletin for Researchers

Bulletin 06 | Research Security Resiliency Team

Research Security & Safety

The Stony Brook University community has many valuable resources to protect. These bulletins are meant to provide quick facts, best practices, and key University contacts.

Receiving Proprietary/Controlled Information

While much of the university's research output is open and unrestricted Fundamental Research, the receipt of certain 3rd party content needs to be securely handled due to export controls.

Why Securing This Information is Important

By properly securing 3rd party proprietary or controlled information, you are taking steps to prevent:

- Inadvertent release of technological know-how to unauthorized foreign persons (a "deemed export") which can have negative impacts on U.S. national security
- Contractual breaches if information is governed by an NDA or CDA
- Financial or administrative penalties upon SBU by the gov't

Best Practices

- Utilize Non-Disclosure Agreements (NDAs) when receiving incoming proprietary information – particularly with industry partners/sponsors
- Work with a university Export Compliance Officer to plan for the appropriate level of physical and IT security if the incoming information is subject to export controls (ITAR or EAR)
- Keep a log of whom within your lab/research group is authorized to have access to the information
- Report any unauthorized disclosures to an Export Compliance Officer immediately!

Whom to Contact

The Export Controls Program (part of the larger Research Security Program) manages all aspects of export compliance for SBU.

They are located within the Office of the Vice President for Research (OVPR) and can be contacted at: ovpr_exports_admin@stonybrook.edu

University Policy

Export Control Policy

Date Published : 8/15/2024

Date of last revision: 8/15/2024