RCRA - Research Security

David Sundvall, Assistant Director Research Security

Ask RCRA May 2023

Why Research Security?

☑ Responsible stewardship of grant/award funds and research deliverables

☑ Protect federally funded research and technology from theft by foreign entities and governments

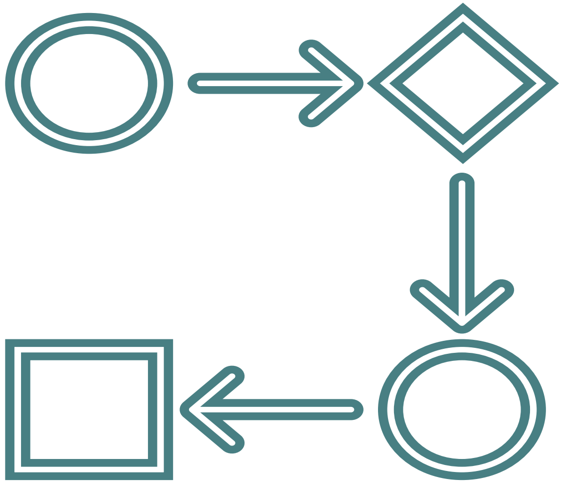
☑ Required by NSPM-33

NSPM-33

1. Disclosure Requirements and Standardization
2. Digital Persistent Identifiers
3. Consequences for Violation of Disclosure Requirements
4. Information Sharing
5. Research Security Programs

Research Security Review Process

- New Faculty Hires
- Visitors (H-1B, J-1, O-1)
- eDisclose (international travel, foreign affiliations)
- Long term international remote work



Research Security Review Information Gathering

1. Visitor name
2. Supervisor name
3. School
4. Country(ies)
5. Disclosures
6. Publications
7. Co-authors
8. Affiliations
9. Awards
10. Proposals
11. Foreign Sponsors
12. Collaborators
13. Lab Staff
14. Bio Sketch
15. Other Current and Pending Support
16. SciENcv
17. ORCID
18. RPS – Restricted Party Screening
19. Unitraker –Australia list of Chinese universities of concern
20. CV
21. Export Controls Office
22. Deemed Exports

Research Security Risk Assessment

- Consistency in Disclosures
- Affiliations of Concern
- International Travel
- Best practices in research data security (data management plan)

Low

Medium

High

Research Data Security Recommendations

- Update and patch hardware and software.
- Use encryption on your devices.
- Use Emory owned and managed devices.
- Minimize the use of personal devices as much as possible.
- A clean loaner laptop should be used for remote access.
- Know what types of data you are collecting, processing, storing, or sharing.
- VPN must be used for remote access.
- When travelling offsite, maintain possession of your devices.
- Avoid travelling with data this isn't necessary.
- Do not plug unknown peripherals into your Emory device.
- Do not download and save to desktop or a local drive.
- Use SharePoint or OneDrive for data storage.
- Know who has access to the data and apply appropriate access restrictions.
- Use strong passwords on devices and folders.
- De-identify data when possible.
- Have a data management plan.
- Securely destroy unneeded data.
- Report hacked, lost, or stolen devices as soon as possible to Emory Security

Questions

For more information:

RCRA

Email: researchsecurity@emory.edu