You Are The First Line Of Defense!

Report Concerns
to **rsp@tamus.edu**

What is Insider Risk In Academic Research?

The potential that a faculty, staff, student, or approved visitor who has, or once had, authorized access to research, data, facilities, equipment, people, or resources may wittingly, or unwittingly, commit acts that resulted in, or might result in, harm through the loss, theft, or misuse of ideas (methods, analysis, results), damage or destruction of equipment, facilities, and resources, or delay of innovative research and appropriate scientific recognition*

What are Indicators of Insider Risk?

- **Unauthorized disclosure of classified, CUI or proprietary information (spills and/or leaks)**
- **Improper use of privileged access**
- **Working odd hours without authorization**
- **Knowingly bypassing technology-associated security rules/protocols**
- **Inappropriate copying of classified, CUI or proprietary information**
- **Requests for technical or program access beyond scope of work**
- **Introduction of unauthorized technical devices into the workplace**
- **Keeping unauthorized backups**
- **Unauthorized requests for, use of, or removal of technical equipment**
- **Hoarding files, data, code, and programs**

What Can I Do?

You can report your concerns to the TAMUS Research Safeguarding Program at rsp@tamus.edu, knowing they will be addressed discretely and with no fear of retribution.

If you are interested in learning more, please refer to TRAINTRAQ course # 2114748: Insider Risk Awareness

TAMUS Research Security Program
RSP@tamus.edu

***Doodson, James, Caputo D.D., Higgins, Bryan, Esposito, Michael, 2023. MITRE Insider Risk Management Program Reference Manual for Higher Education. P. 1-6.**