

RESEARCH BEST PRACTICES FOR PROTECTING SENSITIVE, PROPRIETARY, AND CLASSIFIED INFORMATION ON CAMPUS



The open and collaborative environment of U.S. higher education institutions is a cornerstone of academic freedom and innovation. However, this openness can be exploited by foreign adversaries and competitors seeking to steal intellectual property and sensitive information.



Potential Threats

- ✓ **Theft of Technical Information or Products:** Foreign entities may attempt to steal vulnerable research and technical data.
- ✓ **Bypassing Research and Development Costs:** Adversaries might exploit academic research to avoid the high costs of R&D.
- ✓ **Espionage Recruitment:** Individuals on campus may be targeted for recruitment into espionage activities.
- ✓ **Exploitation of Student Visa Programs:** Foreign nationals may misuse student visas to gain access to sensitive information.



Exploitation Methods

- ✓ **Computer Intrusions:** Cyberattacks aimed at accessing sensitive research data.
- ✓ **Collection of Sensitive Research:** Using students or visiting professors to gather information.
- ✓ **Spotting and Recruiting:** Identifying and recruiting students or professors for espionage.
- ✓ **Unsolicited Emails or Invitations:** Sending phishing emails or invitations to gather information.
- ✓ **Spies for Training:** Sending individuals to gain language and cultural training and establish credentials.
- ✓ **Funding or Establishing Programs:** Creating or funding university programs to gain access to research.



Best Practices

By implementing these best practices, research and higher education institutions can better protect their sensitive, proprietary, and classified information from exploitation and cyber threats.

- ✓ **Use a Password Management Solution:** Use a password manager to create and store strong and unique passwords, such as [1Password](#), available to campus users. Similarly, it is strongly recommended that you implement [multi-factor authentication \(MFA\)](#) on all apps and services that allow it.
- ✓ **Secure Networked Devices:** Ensure all electronic equipment connected to the campus network is secured against unauthorized access by following manufacturer's documentation and restricting incoming access to only necessary ports and protocols.
- ✓ **Cyber Hygiene:** Keep operating systems and applications up to date with patches and security updates. Use anti-virus and anti-malware solutions that automatically update and run regular scans. Avoid using laboratory systems for general computing purposes like web browsing or email.
- ✓ **Data Backup and Security:** Regularly back up data and ensure backups are kept in a secure location and disconnected from the primary network. Test backups frequently to ensure they are complete and functional.
- ✓ **Create an Incident Response Plan (IRP):** an IRP is a structured approach for handling and managing security incidents. Key components include: identifying potential security incidents, measures to contain incidents and prevent further damage, steps to eradicate the cause of the incident, restoring and validating system functionality and conducting a post-incident review.