Faculty (incl. adjuncts and researchers)

Protect course materials, research data, and student records. Lead by example for your students.

Before — prepare

- Enable MFA on every account tied to teaching and research, including grant systems, journals, and cloud collaborators.
- Store research data in approved campus storage with versioned backups. Don’t keep the only copy on a personal laptop.
- Use institution-managed devices when possible, or at minimum follow the IT-provided configuration baseline.
- Encrypt laptops and external drives that contain student data, IRB-protected information, or grant deliverables.
- Verify any external collaboration tool with IT before sharing sensitive data; check vendor security disclosures.
- Treat unsolicited ‘paper invitation,’ ‘co-authorship,’ or ‘grant award’ emails with suspicion — these are common lures.
- Discuss data handling with grad students and TAs; one shared compromised account can expose a whole lab.

During — respond

- If you suspect a phish, stop typing. Verify with IT before clicking anything else.
- If you cannot access your files or see a ransom note, disconnect the device from the network (Wi-Fi off, unplug Ethernet) and contact IT immediately.
- Do not power off the device unless instructed — forensics may need volatile memory.
- Notify any active co-authors and lab members so they can check their access and credentials.
- Pause major data movements or external transfers until IT clears the environment.
- If teaching is affected, communicate via institution-approved channels only; attackers exploit confusion.

After — recover & learn

- Restore from clean backups; do not reuse files from the suspected period without IT validation.
- Review research data integrity: file hashes, version history, and any altered timestamps.
- If student data was exposed, coordinate with the registrar, IT, and legal on FERPA-aligned notification.

- Update your own threat model: which accounts, datasets, and partners are most attractive to an attacker?
- Share lessons in a department meeting; a five-minute brief prevents the next incident.

Self-audit checklist

- ■ MFA is enabled on email, LMS, grant portals, and journal/publisher accounts.
- ■ Research data is in approved storage with automated backups and version history.
- ■ My laptop is encrypted (FileVault, BitLocker, or campus-managed equivalent).
- ■ I know how to report a phishing email and who to call for an active incident.
- ■ Lab/TA/RA accounts follow the same MFA and backup standards as mine.
- ■ External tools used in my courses or research have been checked with IT.
- ■ I have a written plan for what happens to my course if the LMS is unavailable for 48 hours.