WELCOME TO OUR DECEMBER RCR TRAINING

- Please make sure your microphones are muted
- There will be a Q&A session after this presentation
  - Please reserve your questions until then
    OR
  - Put any/all questions in the chat and we will address them after the presentation
- This session will be recorded

UNE

INNOVATION FOR A HEALTHIER PLANET

1

YOUR HOST FOR THE DAY!

- Yefrenia Henriquez Taveras
  - MPH, MHA, CHES, CIP
  - Public Health & Research Compliance Specialist
  - Sociobehavioral and Biomedical Research Expertise
  - UNE IRB Compliance Coordinator

UNE

INNOVATION FOR A HEALTHIER PLANET

2

Data Security in Research

December 19, 2023

Yefrenia Henriquez Taveras, MPH, MHA, CHES, CIP
IRB Compliance Coordinator
Office of Research & Scholarship
yhenriqueztaveras@une.edu

UNE

INNOVATION FOR A HEALTHIER PLANET

3

OBJECTIVES

- Highlight the significance of protecting data in research contexts, discussing potential risks and consequences of data breaches or misuse.
- Explain the university's specific policies and guidelines for securing research data, including any legal or regulatory requirements.
- Provide practical guidance on how to secure research data effectively, including methods for encryption, access control, and secure data storage and transmission.
- Explore the ethical implications of data security in research and the importance of compliance with university policies and external regulations.
- Identify resources and support systems available within the university for researchers to implement effective data security measures, including training programs, IT support, and reporting channels for security incidents.

UNE

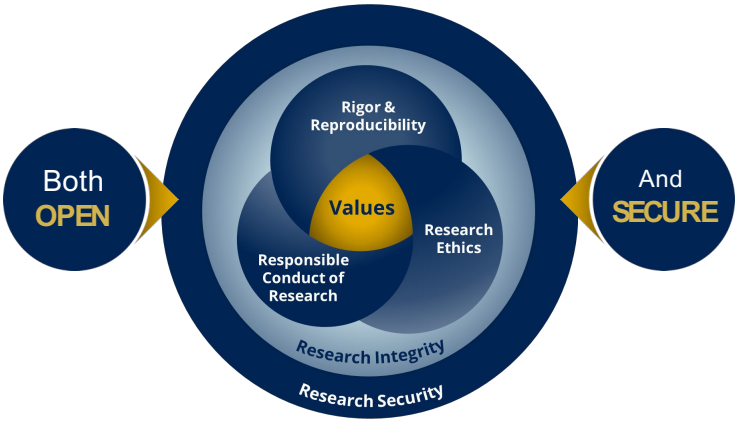
INNOVATION FOR A HEALTHIER PLANET

4

Background

5

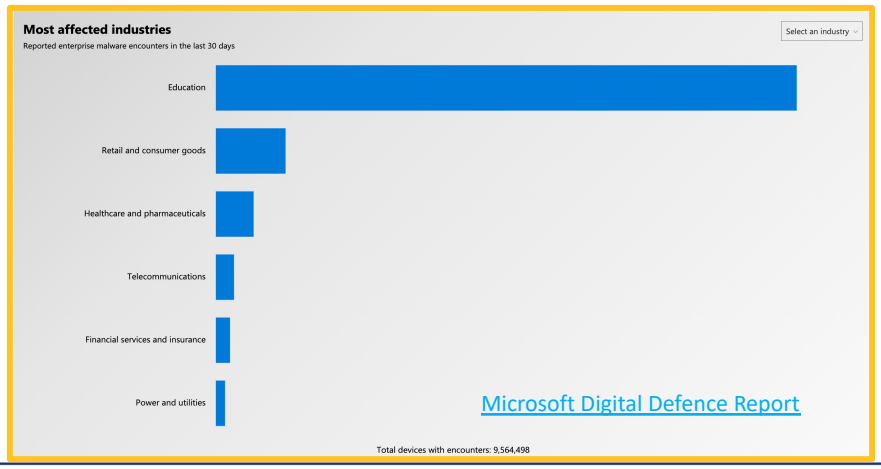
RESEARCH SECURITY & HIGHER EDUCATION



Job Hindrances	• Loss of access to campus computing network • Inability to access files and do work
Data Loss	• Loss of confidentiality and integrity • Loss of valuable university info or research • Compromised personal data
Disciplinary Actions	• Lawsuits • Loss of public trust • Loss of grant opportunities • Prosecution • Internal disciplinary action • Termination of employment

6

HIGHER EDUCATION AS A TARGET FOR HACKERS



Microsoft Digital Defence Report

7

CYBERATTACKS CASE STUDIES: THE COLLEGE THAT SHUT DOWN PERMANENTLY AFTER A RANSOMWARE ATTACK

- **Who was hacked:** Lincoln College in Illinois, which opened in 1865 and qualified as a predominantly Black institution under the Department of Education
- **The attack:** In May of 2022, Lincoln College was hit with a ransomware attack that they were unable to recover from. While the pandemic contributed to the shutdown, with students opting to defer enrollment or take a leave of absence, the school was the first to close partly because of a ransomware attack.
- The cyberattack rendered critical systems inoperable, such as those used for fundraising, recruitment, retention, and enrollment, and blocked institutional data.
- **The takeaway:** This particular ransomware attack made it impossible for the school to access their computer systems and data, which they could not afford to replace. If possible, higher learning institutions should join the Research Education Networking Information Sharing and Analysis Center (REN-ISAC) to stay up to date on cybersecurity threats and risk management.
- Compromised passwords are often hackers' way in to carry out a ransomware attack. Strengthening passwords across your organization can stop these attacks before they start.

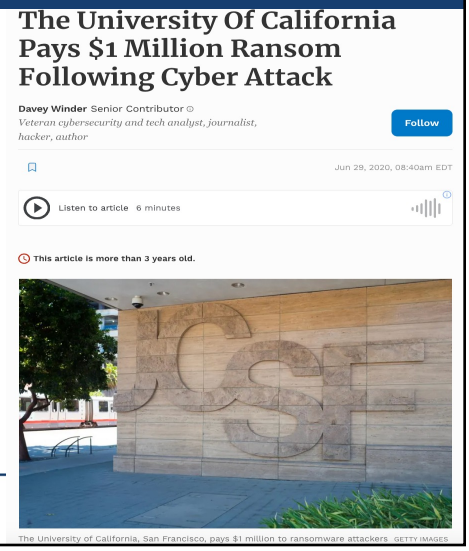
Illinois college, hit by ransomware attack, to shut down

Lincoln College, which broke ground in 1865, is one of only a handful of rural American colleges that qualify as predominantly Black institutions by the Department of Education.

8

CYBERATTACKS CASE STUDIES: THE RANSOMWARE ATTACK THAT COST $1.14 MILLION

- **Who was hacked:** University of California, San Francisco (UCSF)
- **The attack:** NetWalker, a group of ransomware operators, went on a ransomware spree in 2020, targeting universities. Through "brute force attacks"—trial and error password attempts by bots—NetWalker gained access to sensitive data, and threatened to expose the data if the universities failed to pay the ransom. One of the most affected by this double extortion scheme was UCSF, who paid $1.14 million in ransom to recover crucial data tied to the medical school's academic work.
- **The takeaway:** There are ways to protect against a brute force attack, including using passwords with the maximum amount of characters for sensitive accounts. The longer the password, the longer it would take for software to "guess" it and the less likely cybercriminals are to succeed.
- Enabling multifactor authentication for your accounts, in addition to creating long, secure passwords, is crucial.



The University Of California Pays $1 Million Ransom Following Cyber Attack

Davey Winder Senior Contributor
Veteran cybersecurity and tech analyst, journalist, hacker, author

Follow

Jun 29, 2020, 08:40am EDT

Listen to article 6 minutes

This article is more than 3 years old.

The University of California, San Francisco, pays $1 million to ransomware attackers GETTY IMAGES

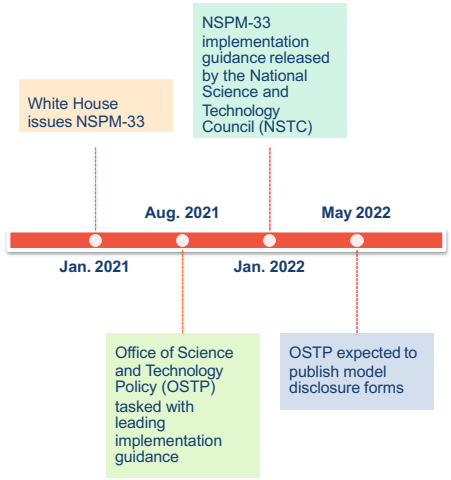
9

Federal Directives

10

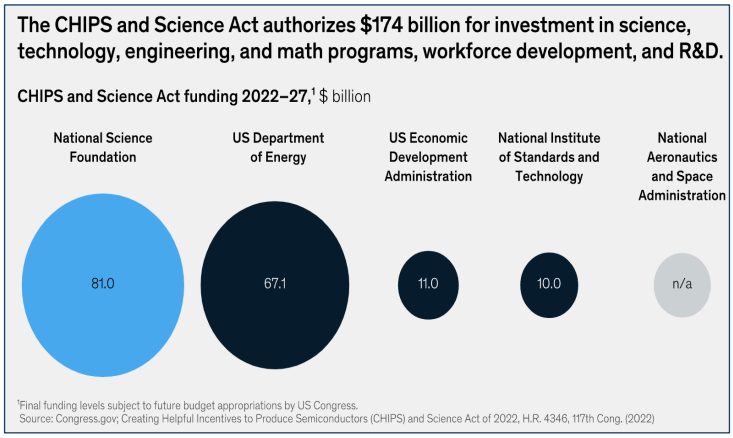
NATIONAL SECURITY PRESIDENTIAL MEMORANDUM-33 (NSPM-33)

- Presidential directive requiring federal research funding agencies to strengthen and standardize disclosure requirements for federally funded awards.
- The National Security Presidential Memorandum 33 (NSPM-33) also requires major institutions (≥$50M/year) receiving federal funds to establish research security programs.
- Research Security Programs within research organizations, that include:
  I. Cybersecurity
  II. Foreign travel security
  III. Research security training
  IV. Export control training



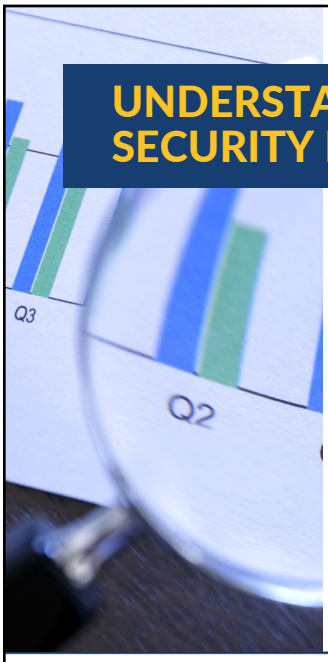
THE CHIPS AND SCIENCE ACT OF 2022: RESEARCH SECURITY

- The CHIPS and Science Act includes several research security provisions, including:
  - Prohibition of malign foreign government talent recruitment programs
  - ***Requirement to establish a Research Security and Integrity Information Sharing and Analysis Organization (RSI-ISAO)***
  - Research security training requirement for all covered personnel
  - Inclusion of research security training as part of Responsible and Ethical Conduct of Researchtraining
  - Reporting on foreign financial transactions and gifts



UNE Policy Research Data and Security, Research Materials Management, Sharing, and Retention

13



UNDERSTANDING UNE'S RESEARCH DATA AND SECURITY POLICY

- The policy sets expectations for the management, sharing, and retention of Research Data and Materials at UNE.
- Aims to meet evolving sponsor and publisher expectations for data sharing.
- Ensures UNE's commitment to research transparency and replicability.
- Asserts UNE ownership over all Research Data and Materials produced with University resources.

14

KEY DEFINITIONS AND POLICY SCOPE

- **Data User:** Researchers or personnel involved with Research Data/Materials at UNE.
- **Research Data:** Information necessary for reconstructing and evaluating research results.
- **Research Materials:** Tangible products of research or items used in research processes.
- **Source Data:** External data used for UNE research, obtained via proper agreements.
- *Policy applies to all UNE community members handling Research Data/Materials.*

UNE

INNOVATION FOR A HEALTHIER PLANET

15

WHOM DOES THIS POLICY APPLY TO?

- ***All members of the UNE community!***
  - Faculty, staff, students, visiting scholars, and postdoctoral fellows,
  - Any other persons involved in the creation, acquisition, access, use, management, sharing, retention, and destruction of Research Data and Research Materials at or on behalf of UNE
- The policy *does not distinguish between funded and unfunded efforts, except where specific sponsor requirements prevail.*

UNE

INNOVATION FOR A HEALTHIER PLANET

16

POLICY STATEMENT AND AUTHORITY

- UNE supports academic freedom and responsible research dissemination.
- Researchers must adhere to ethical standards and agreement terms regarding data use and disclosure.
- The Provost is the final authority on policy compliance, with the Associate Provost for Research and Scholarship (APRS) as the subject matter expert.

OWNERSHIP AND STEWARDSHIP OF DATA

- UNE retains ownership of Research Data/Materials, except as otherwise specified by sponsor terms.
- Data Users are responsible for proper management, sharing, and protection of Research Data/Materials.
- PIs have rights to access and copy their data upon departure from UNE:
  - Departing Faculty Checklist: https://www.une.edu/research/policies-and-forms
  - Laboratory notebooks may not be taken from UNE by any party departing UNE

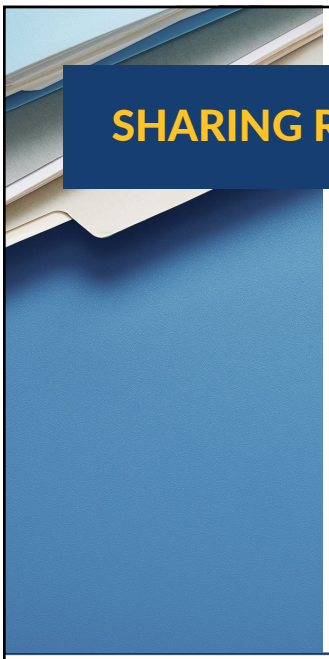
ENSURING DATA SECURITY

- Researchers must identify data security obligations and ensure appropriate protection.
- UNE provides a risk-based approach to data categorization and security standards.
- Data Users must comply with data risk classifications and implement corresponding security controls.
- ITS is available to assist researchers with risk self-classification and can be contacted at CIS-datasecurity@une.edu

UNE

INNOVATION FOR A HEALTHIER PLANET

19



SHARING RESEARCH DATA AND MATERIALS

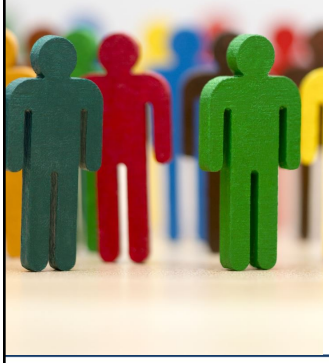
- Responsible sharing of Research Data is encouraged to support transparency and reproducibility.
- Researchers must document re-use stipulations and comply with sharing agreements like Data Use Agreements.
- UNE provides infrastructure for data preservation and recommends DUNE:DigitalUNE for long-term retention.

UNE

INNOVATION FOR A HEALTHIER PLANET

20

RETENTION OF DATA



- Standard retention period is three years post-study completion or after the final expenditure report.
- Longer retention required for intellectual property protection, ongoing litigation, or compliance with specific regulations.
- PIs are responsible for data selection and compliance with retention and destruction requirements.
- ITS will work with the PI to determine the most appropriate disposal solution for electronic data that has met and/or exceeds the data retention periods outlined within this policy.

UNE

INNOVATION FOR A HEALTHIER PLANET

21

RESPONSIBILITIES OF INVESTIGATORS (DATA USERS)

- **Primary Responsibility**: PIs hold primary accountability for stewardship of Research Data and Materials.
- **Data Management**: Must collect, record, manage, retain, and share Research Data and Materials in accordance with UNE policies and legal requirements.
- **Data Retention**: Ensure original data is retained as per policy guidelines.
- **Confidentiality**: Maintain confidentiality and protect Research Data, especially human subject data, as per protocols.

UNE

INNOVATION FOR A HEALTHIER PLANET

22

RESPONSIBILITIES OF UNE

- **Rights Protection**: Safeguard the rights of UNE researchers, including academic freedom and data access.
- **Policy Implementation**: Develop and implement policies for compliance with legal and sponsor requirements.
- **Infrastructure Support**: Provide secure systems for maintaining Research Data and Materials.
- **Data Security**: Offer guidance and support for data security and manage secure infrastructure for research.

UNE

INNOVATION FOR A HEALTHIER PLANET

23

COMPLIANCE AND VIOLATIONS

- All UNE community members must familiarize themselves with and follow this policy.
- Violations must be reported to the Policy Owner or Contact.
  - Associate Provost for Research and Scholarship
- Consequences of non-compliance range from suspension to termination.

UNE

INNOVATION FOR A HEALTHIER PLANET

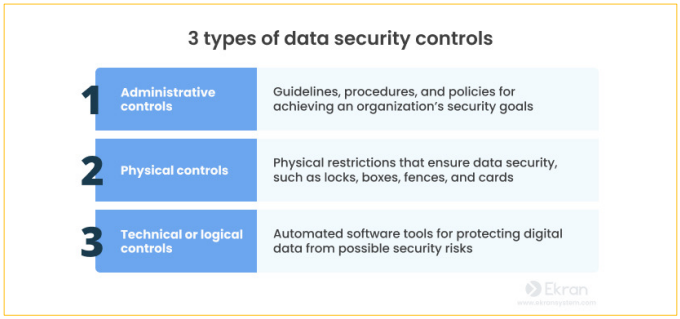
24

Best Practices for Research Data Security

25

SAFEGUARDING INFORMATION

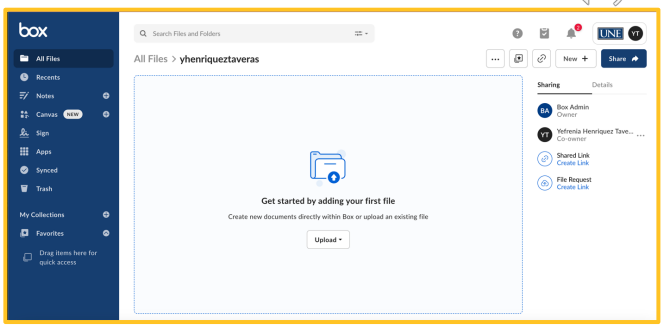
- Understanding Research Data Sensitivity
- Secure Data Storage and Handling
- Data Analysis Security
- Device Management
- General Practices: PHI
- Institutional Frameworks
- Compliance and Ethics



26

USING BOX

- BOX serves as the central system for securely storing and sharing UNE documents, both internally and externally.
- Accessing BOX via Okta.une.edu
- Provides a personal folder, similar to a U: drive, for private access or sharing.



Email helpdesk@une.edu for any questions about set up and usage

27

Small Actions: Cybersecurity Tips

28

Cybersecurity Tip # 1

Add passcode protection and expiration dates when sharing links to recorded Zoom meetings, and/or files.

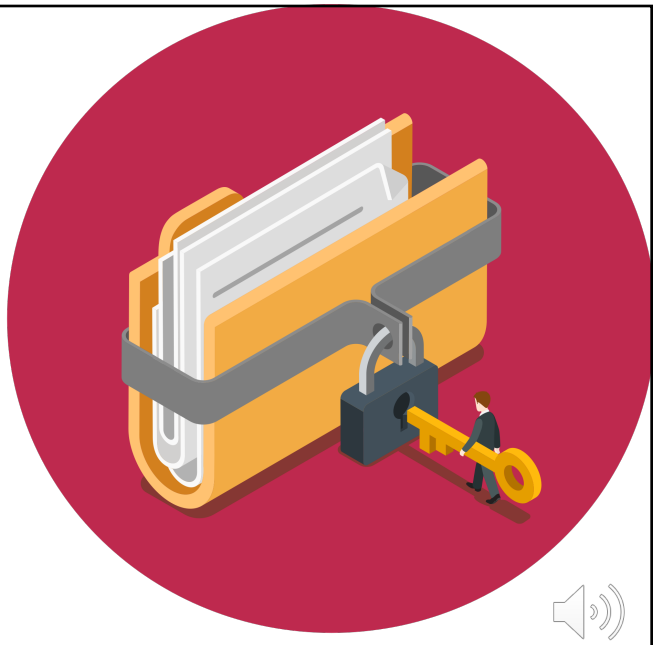
UNE

INNOVATION FOR A HEALTHIER PLANET

29

Cybersecurity Tip # 2

Store sensitive data in UNE-managed locations, like BOX, OneDrive or SharePoint.



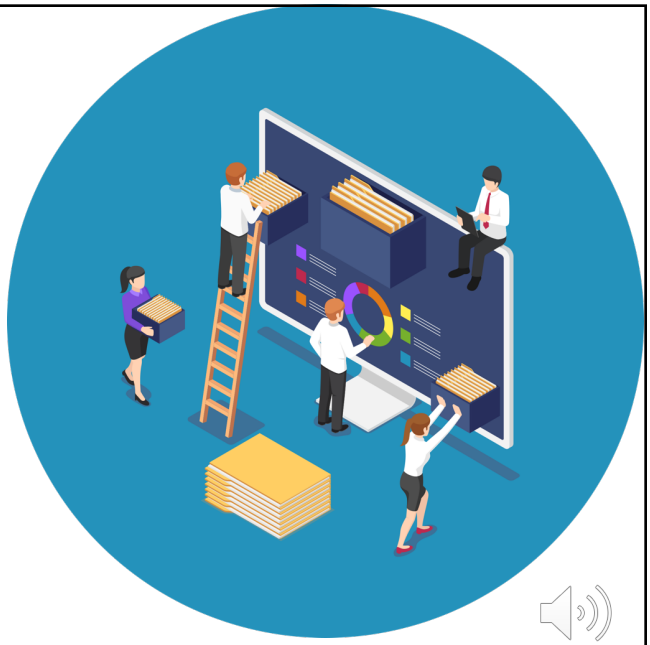
UNE

INNOVATION FOR A HEALTHIER PLANET

30

Cybersecurity Tip # 3

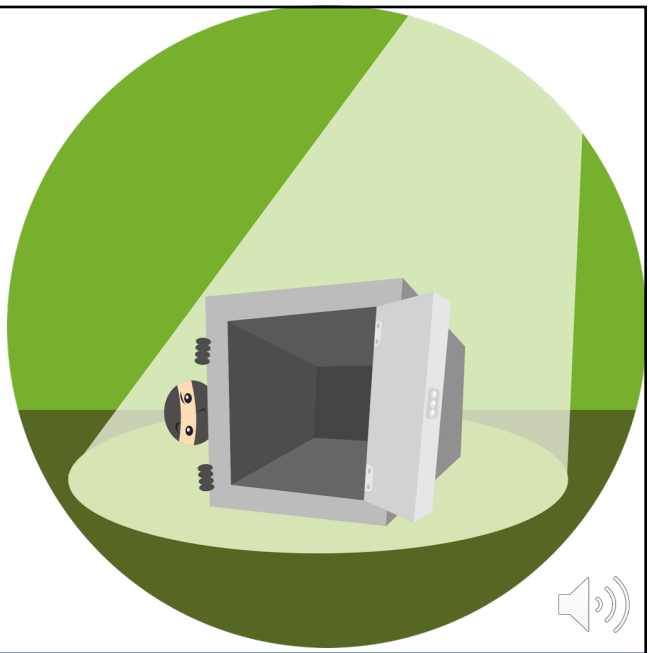
Keep your team on the same page and protect your data. Send links instead of files when sharing with your team.



Cybersecurity Tip # 4

Thieves can't steal files that aren't there.

Protect the data you need, delete the data you don't.



Cybersecurity Tip # 5

Use the BOX or OneDrive apps to securely scan documents to the cloud with a simple tap.

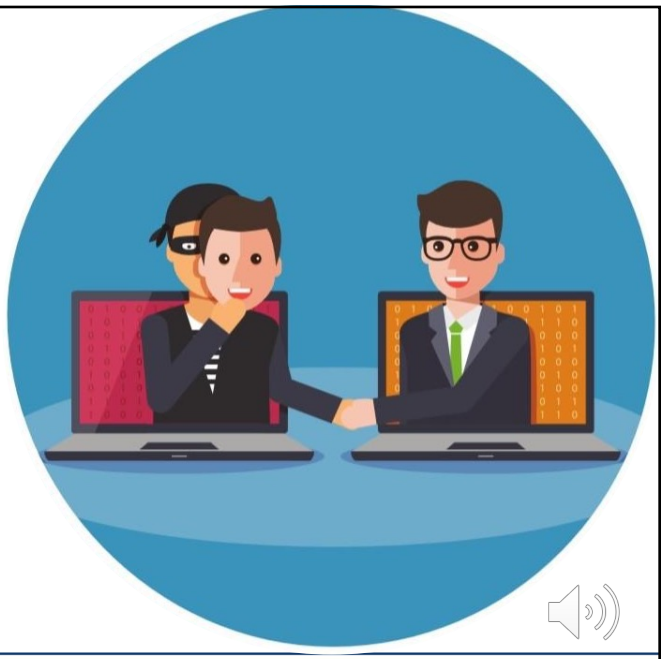
UNE

INNOVATION FOR A HEALTHIER PLANET

33

Cybersecurity Tip # 6

Is that really you?
If you get an odd request from someone you know, verify it by phone call or text.

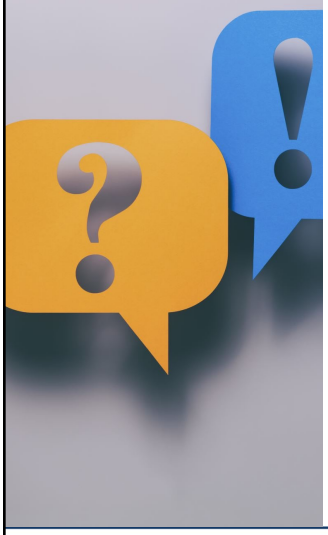


UNE

INNOVATION FOR A HEALTHIER PLANET

34

FAQS



- **Why does UNE own my research data and research materials?**

UNE is the owner of all research data and research materials for projects conducted at the University, under the auspices of the University, or with University resources (monetary or otherwise). In addition, the institution must ensure that its community complies with laws, regulations, and institutional policy, including, for example, assessing allegations of research misconduct. Ownership concerns the rights and title to the research data and research materials, not physical possession nor direct responsibility.

- **Can a department have a policy about data ownership that overrides this policy?**

Departments within the university cannot override this policy. The only exception to this rule is when UNE's ownership is specifically precluded by the terms of sponsorship or other agreements.

- **Who is responsible for the storage of research data?**

The Principal Investigator is responsible for developing and overseeing a research data storage plan that is in accordance with the appropriate data classification (UNE Data Security Guidelines).

- **Who should I contact if I have questions about research data or research material sharing between UNE and an external entity?**

In some instances, sharing research data external to UNE may require a Data Use Agreement. Similarly, sharing research materials outside of UNE may require a Material Transfer Agreement. For Data Use Agreement or Material Transfer Agreement assistance, email osp@une.edu.

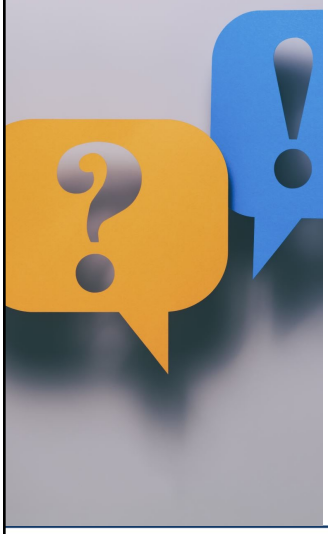
In all cases, if research data are being shared under an IRB-approved human subjects research protocol, the Principal Investigator should adhere to the data sharing procedures outlined in the approved protocol and contact the UNE IRB with any questions at IRB@une.edu.

UNE

INNOVATION FOR A HEALTHIER PLANET

35

FAQS, CONT.



- **I have a Data Use Agreement that requires I destroy the data I received before the retention period required by my sponsor. What do I do?**

Data collected from an external party under a Data Use Agreement is considered Source Data (see the policy for a full definition). Source Data must be destroyed in accordance with the terms of the Data Use Agreement; this is permissible under the approved policy.

- **What's the difference between anonymous and confidential data?**

An individual's participation in a research project can be described as ***anonymous*** if it is impossible to know whether that individual participated in the study. For example, participation in an online survey would be considered anonymous if that survey could not be linked in any way to the individual.

When participation is ***confidential***, the research team knows that a particular individual has participated in the research, but the team members are obligated not to disclose that information to others outside the research team, except as clearly noted in the consent document.

- **What are public-use data files?**

Public use data files are files from which all PII has been removed and the data are coded in such a way as to make identification of research subjects extremely unlikely. Researchers who work with public use data sets that do not contain PII may not meet the regulatory definition of research involving human subjects. However, some restricted use agreements nevertheless require local IRB review. As such, researchers are encouraged to consult the Institutional Review Board to determine if their proposed research requires IRB review.

- **What are UNE's guidelines for retaining data on its infrastructure, and what are the secure storage options available?**

For retention purposes, any data that must continue to remain on UNE infrastructure should be kept in UNE's secure data center on its encrypted SAN or in UNE's secure Collaborative space BOX.

UNE

INNOVATION FOR A HEALTHIER PLANET

36

RESOURCES

Privacy
- **Phone** _ 646-962-6930
- **Email** _ **hipaa@une.edu**
- **Website** _ **https://www.une.edu/research/integrity/hipaa**

Security
- **Phone** _ 646-962-3010
- **Email** _ **CIS-datasecurity@une.edu.**
- **Website** _ **https://www.une.edu/its**

Hotline
- **Phone** _ (866) 587-6636
- **Website** https://www.une.edu/hotline-policies-and-procedures

UNE's policy prohibits retaliation for reporting concerns related to compliance and privacy.

UNE

INNOVATION FOR A HEALTHIER PLANET

37

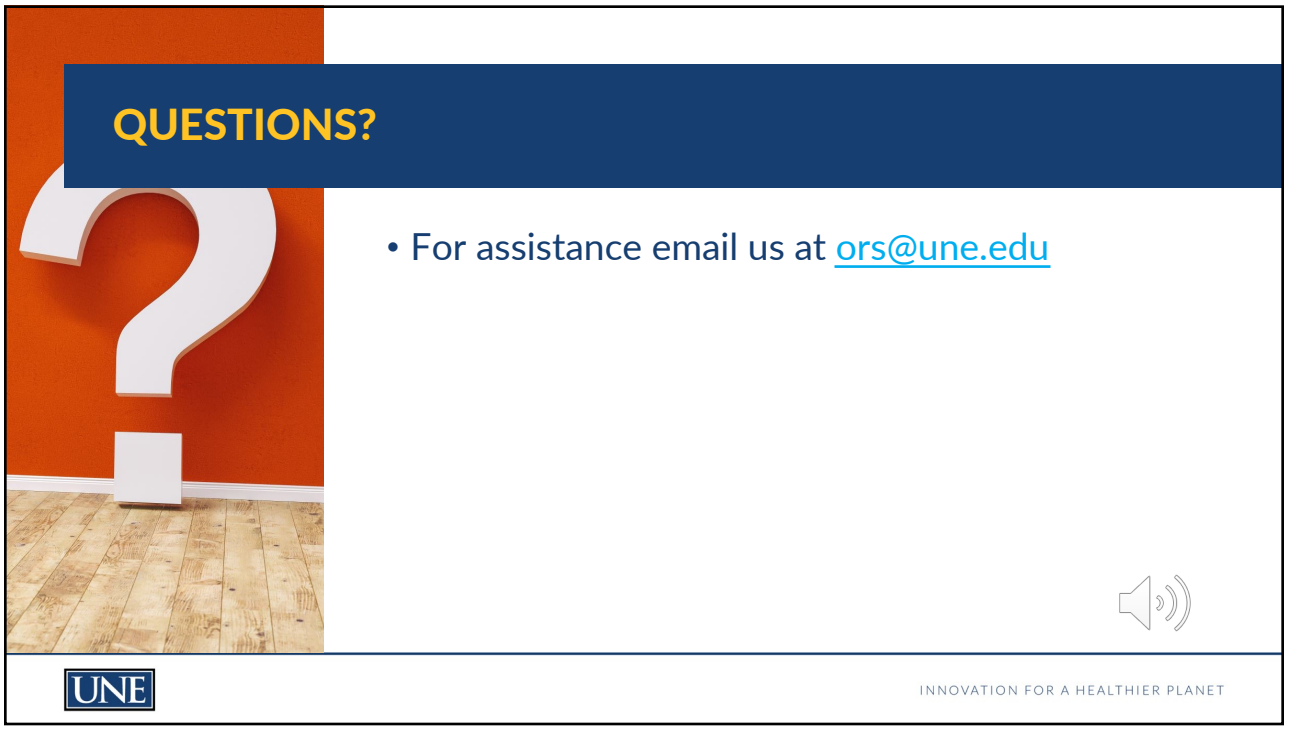
RELATED POLICIES AND INFORMATION

- UNE Policy on Research Data and Security, Research Materials Management, Sharing, and Retention
- University of New England Acceptable Use Policy
- University of New England Data Risk Classifications
- University of New England IP policy
- DUNE: DigitalUNE - UNE's Digital Repository
- National Institutes of Health Sharing Policies
- National Science Foundation Data Sharing Policy

UNE

INNOVATION FOR A HEALTHIER PLANET

38


QUESTIONS?
• For assistance email us at ors@une.edu
UNE
INNOVATION FOR A HEALTHIER PLANET

39