

# Information Security in Higher Education

Baby Steps

# Dr. Kees Leune CISSP, GCIH, CISM

Information Security Officer at Adelphi University

Email: [kees@leune.org](mailto:kees@leune.org)

Blog: <http://www.leune.org>

Twitter: @leune

# Adam Dodge, CISSP, MSIA

Information Technology Security Officer at Eastern Illinois University

Email: [adam@adamdodge.com](mailto:adam@adamdodge.com)

Blog: <http://www.adamdodge.com/esi>

Twitter: [@adamdodge](https://twitter.com/adamdodge)

# Setting the Stage

Many "fundamental truths" for information security management do not apply in institutes for research and higher education, forcing us to rethink how to protect information.



*Image owned by Radiospike Photography*

# Key Players In Higher Ed

Administration  
Staff  
Faculty  
Students  
Parents of students  
Government  
Third parties



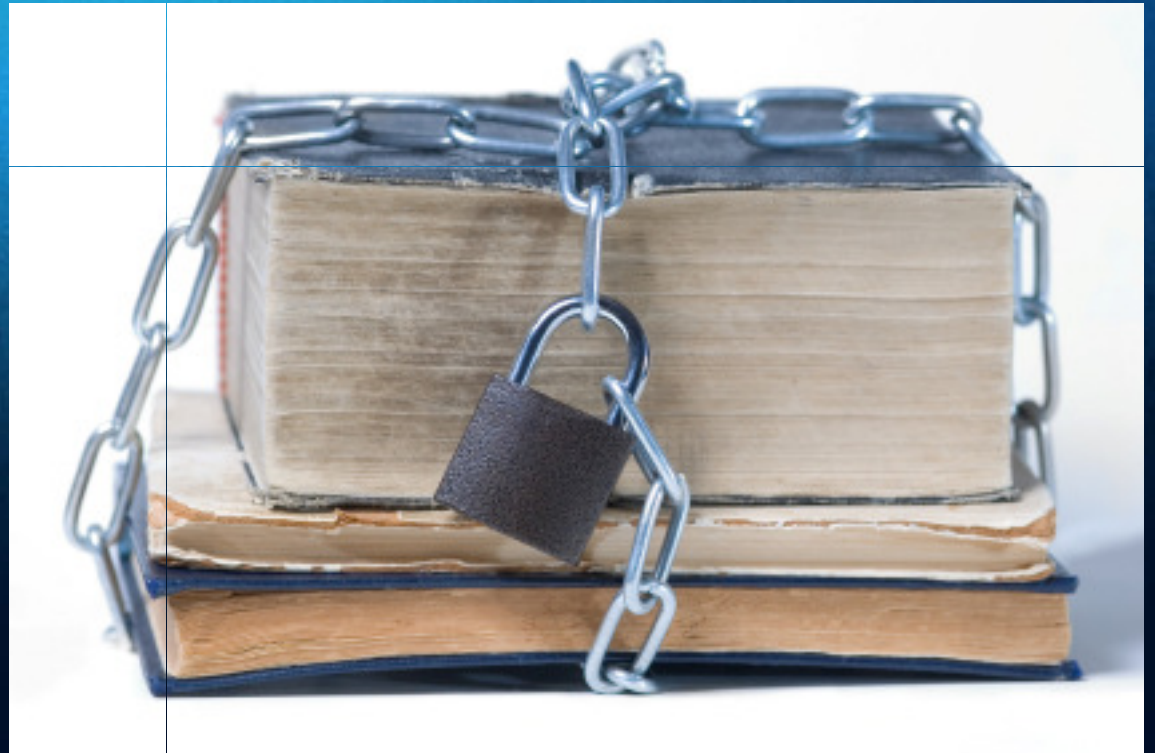
# Issue 1: Intellectual Property

## *Copyright*

- Typically owned by the faculty member who creates it.
- Work performed by students often retained by supervisor.

## *Patents*

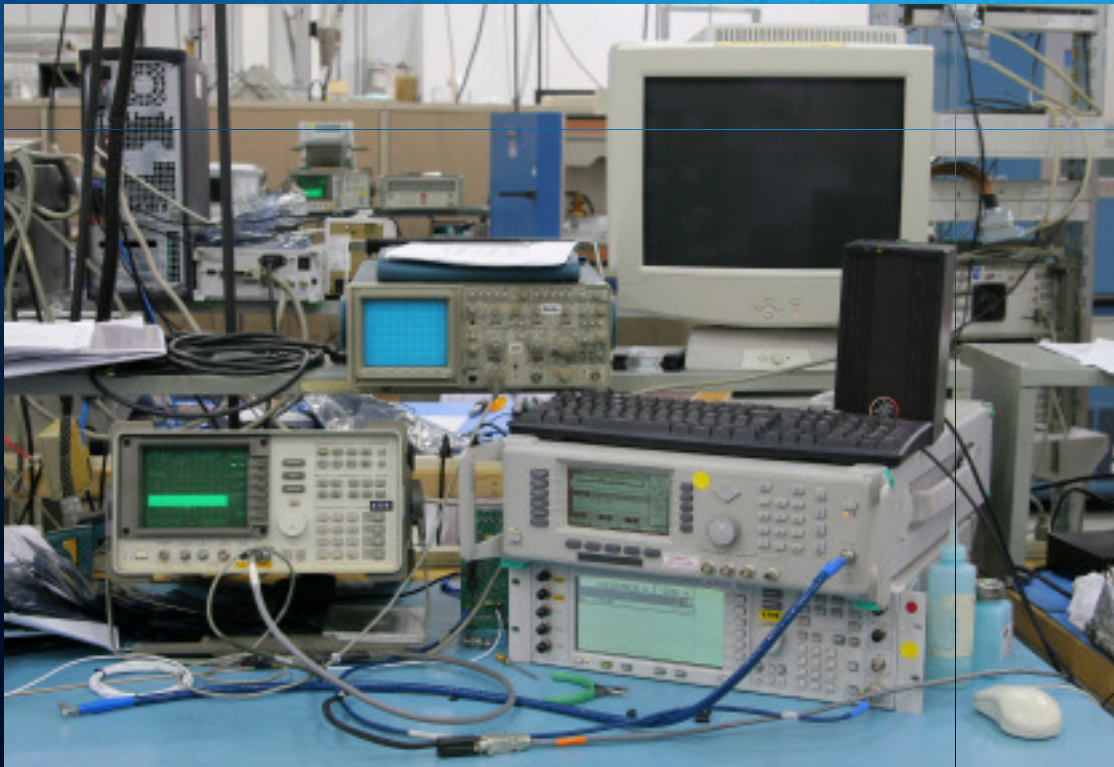
Regularly retained by the University with a revenue-sharing agreement with the faculty member(s) involved.



# Issue 2: Academic Freedom

## *Reasonable Expectation of Privacy*

The Freedom of Academic Pursuit grants members of faculty a reasonable expectation of privacy.



## *Tenure*

Offers a level of protection unparalleled in commercial environments.

# Issue 3: Open Networks

## *High Speed Networks*

- Must serve academic and residential uses
- Few, if any, restrictions

## *Few Restrictions on Equipment*

- Tend to have a mix of new and old equipment
- Faculty often need various tools for academic purposes



# Issue 4: Decentralized Environment

## *Lack of Central Control*

- Generally control of resources split between central IT, academic IT, and individuals running stand-alone servers
- Grants and sponsored research have own rules



## *Third Parties*

Often information housed on systems not controlled by college/university

# Lesson 1: Know Your Customer

## *Three Distinct Groups in Higher Ed*

- Each has access to different types of information
- Each must be handled differently

## *Approaching These Groups*

- Know what concerns each group
- Know how to engage each group

# Lesson 2: Information Security Has No Place in Traditional Academic Environment

## *Free and Open Exchange Is the Goal*

- Communication between faculty and students is central to the mission

## *Residence Hall Networks Have Unique Challenges*

- Students in residence are de facto renters
- Increasing government regulations lead to residence hall network activity creating risk to institution

# Lesson 3: Higher Education Is Unique Because of Academic Freedom

## *Faculty Are Self-Governing*

- Freedom to choose research topics without control or censorship
- Allowing such freedom limits amount of control by institution

## *Ownership of Work Does Not Always Belong to Institution*

- Faculty/Researcher determines who has access and how that access is to be granted
- Framework for user-centric controls must be implemented

# Lesson 4: Higher Education Is Not Unique Because of Business Data

## *Administrative Functions Are the Same as Any Organization*

- Accounts Payable, Human Resources, payroll, investments, etc.
- Point of sale and health care functions also exist outside of traditional academic role

## *Large Number of Non-Academic Regulations Must Be Met*

- Required controls can easily conflict with regulatory requirements
- Number of regulations increasing due to funding sources and court cases

# Lesson 5: Balance Guidance and Control

## *Decentralization Is a Good Thing*

- Size and scope of college and university information resources makes centralized control very difficult
- Distributing control allows the distribution of authority and responsibility

## *Strong Central Guidance Is Key*

- Create guidelines, goals and objectives for resource owners
- As with everything here, the goal is baby steps

# Lesson 6: Focus on Response, Rather than Prevention

## *Implement State-of-the-Art Incident Response*

- Need-to-know, least-privilege and ubiquitous monitoring cannot be universally applied
- Be prepared to quickly and adequately respond to incidents, but keep in mind the different containment and enforcement options for different stakeholder groups
- Form a CSIRT (Computer Security Incident Response Team) with buy-in from student judicial officer, provost, registrar, and other key stakeholders

# Putting It All Together

*Information Security in Higher Education is not very different from other environments, but:*

- Intellectual property issues may be considered differently in higher education than in most commercial/government organizations
- Stakeholders will have a much higher degree of autonomy:
  - need-to-know, least-privilege, and ubiquitous monitoring cannot be universally applied
- Security management will be driven by incident response in a higher degree than in other environments
- Be ready to find some odd stuff

# Questions?

[kees@leune.org](mailto:kees@leune.org)

[adam@adamdodge.com](mailto:adam@adamdodge.com)