IST346:
Information Ethics

Ethics

- **Ethics** are the principles of conduct that govern a group of people.
  - Ethics are not morals.
  - **Morals** are the proclamation of what is right and good.
- The boundary between what is and is not ethical is usually blurry….
  - Not because people lack a moral compass
  - But because the organization does not have clear policies

Why discuss Ethics?

- SA's have privileged access to information
  - User's Email and Files
  - Customer financial data
  - Employee confidential data
- "With great power comes great responsibility."
- You need to be able to trust yourself with that responsibility
- You need to be able to question others who ask you to use your privileged access

A cue from the Medical Community: “Informed Consent”

- Informed
  - Knowing your options
  - Knowing the benefits and drawbacks of those options
- Consent
  - Getting permission from the user or granting body
- Bottom line:
  - Inform the users affected then ask for consent, if required.
  - Example: Doctor asks a patient whom they can share their medical records with, inform them that they are granting consent to pass along ANY information to these individuals.

Professional Organizations Codes of Ethics

- Association for Computing Machinery (ACM):
  - https://www.acm.org/code-of-ethics
- League of Professional Systems Adminsitrators (LoPSA)
  - https://lopsa.org/CodeOfEthics
- American Library Association (ALA):
  - http://www.ala.org/tools/ethics
- IEEE:
  - https://www.ieee.org/about/corporate/governance/p7-8.html
- Association for Information Systems (AIS):
  - https://aisnet.org/page/ISEthics
- Academy of Management:
  - https://aom.org/About-AOM/AOM-Code-of-Ethics.aspx

What's Covered?

- Professionalism
- Personal Integrity
- Privacy
- Laws and Policies
- Communication
- System Integrity
- Education
- Responsibility to Computing Community
- Social and Ethical Responsibility

Network/Computer User Code of Conduct

- Policies help to define the ethical boundaries of the organization.
- Acceptable Use Policy
  - Is personal use of company equipment permitted? When?
  - Are there certain types of personal use that are forbidden?
  - Is the AUP location dependent? Time dependent?
  - Personal email from a company email address?
- Network Monitoring Policy
  - Explain services are monitored and logged as part of their administration
  - Information in the logs might be a privacy concern.

Privileged Access Code of Conduct

- People with privileged access (can see other people's otherwise private information) need a special code of conduct.
- People with privileged access should be
  - trained in ethics
  - well versed in User code of conduct, policy and procedure
  - required to accept the CoC before obtaining access

Three Rules of Privileged Access

1. Be careful. Think before you type.
2. Be mindful of and respect the privacy of others.
3. If you mess up, let your supervisor know right away.

- It is better to be honest and up front about any situation.
- “Honesty is the best policy.”

Getting caught in the middle

- What if you catch someone doing something unethical?
  - Eg. You know someone is pirating software at your company.
- What if you're asked to perform an unethical activity?
  - Eg. A Co-worker asks for someone else's files.
- In all cases
  - Verify the request. Get clarification
  - Keep written records of all your activity
  - When in doubt, get clarification. From HR, your supervisor, a lawyer.
  - Change names to protect the innocent when discussing the situation with others.
  - Try to convince people doing unethical activity to confess.

Information Ethics Examples

Example 1 “You’ve been hacked!”

- Dave the SA plays a prank on his co-worker Steve. He sends a direct computer message (something SA’s can do) to Steve computer with the text “you’ve been hacked!” Believing the message is legitimate, Steve reacts accordingly, changing his passwords and notifying the rest of the SA team of the incident. Shortly after Dave let’s everyone know is was a joke and they all share a laugh over the “incident”.

- What is the ethical problem?
- If you supervised these individuals, how would you handle this situation?

Example 2 “I wish I didn’t know that.”

- While trying to diagnose a server problem, you discover Gigabytes of pirated Movies and Music on your server’s hard drive. Thinking it might be a hack you investigate further, only to find the files belong to a co-worker.

- What is the ethical problem?
- How would you handle this situation?
- Can policy help in this situation?

Example 3 “A sales opportunity”

- You’re the lead SA for your company. You’ve been approached by the manager of the sales department (Mary). She is requesting access to one of her staff’s email accounts (Tom) so she can assist in closing a big sales deal while Tom’s on vacation.

- What is the ethical problem?
- What would you do in this situation?
- Does a supervisor have the right to access her employee’s email?
- Can policy help in this situation?

Example 4 “The moral dilemma”

- You are the director of Information Technology for your company. One of your staff from the helpdesk (John) has come to you with a problem. A VP (Tim) brought his notebook in for maintenance, complaining his computer was “sluggish.” When John inspected the computer he stumbled upon sexually explicit material. Though the material is not illegal, it is a violation of the company’s terms of use for IT

- What is the ethical problem?
- What would you do in this situation?
- Do you believe John acted ethically?