UA Policy Critique

The Good, the Bad and the Vague

Definitions

- Information Resource: Information systems and information networks controlled by the university, as well as the information contained or transmitted therein. This applies to all IR acquired and controlled by university or employees.
- User: Anyone who uses an information resource.

- Network: Data transmission Equipment
    - Does not include end user devices such as computers, printers, etcetera.
- Private information: Information that is labeled with the users name and is designated private or is placed in an area for exclusive use by that user
- Sensitive information: Same as above but designated sensitive, but to which a supervisor may need access under unusual circumstances.

Explicit Do’s and Don’ts

You are allowed to do it unless they say otherwise

Authorization must be obtained from personnel with authority to manage the information resource.

Be a responsible user

-Limit resource usage to reasonable levels

Encrypted data should be accessible to authorized users in extenuating circumstances

Prohibited Activities

- Activities cannot violate UA policy at large
- Harassment is a no-no
- Any form of copyright violation or plagiarism
- Unauthorized modification of data
- Anonymous or forged e-mail
- Any attempt to bypass in place security

Content Restrictions (02.07.052)

- Public forums may be restricted on content, not viewpoint
- Harassing messages may be restricted or removed
- Guidelines may be formed for large mailing lists
- Activities that use large amounts of resources may be restricted.

x Apparent endorsement of commercial entities

x Content which is prohibited by law

Admin Do’s and Don’ts

- Must maintain integrity and confidentiality of information resources
- Cannot browse files or view transmissions except at required in line of duty

Enforcement

- Employees may be subject to disciplinary action including termination
- Students may be subject to disciplinary action including expulsion
- Access to information resources may be restricted
- Criminal prosecution may be pursued if applicable.

Fuzziness and Uncertainty

- (Dangerously?) Old regulations (01-31-01)
- No specific definitions of illegal network traffic types
  - Port scanning?
  - Ping sweeps?
  - What is disproportionate or debilitating?
- Most policies refer to employees, not students (R02.07.051 B)

Confusing Rules

- UAF: sharing connections
  - No spouses or children?
- Contradiction
  - UAF and UA: accept responsibility for sharing password
  - Federal: Violation of law