POLICY TITLE	Monitoring and Review of Employee Electronic Communications or Files	**Policy Number**	446
Section	Facilities, Operations, and Information Technology	**Approval Date**	October 14, 2004
Subsection	Information Technology	**Effective Date**	October 14, 2004
Responsible Office	Office of the Vice President of Information Technology		

1.0 PURPOSE

2.0 REFERENCES

2.1 *Freedom of Information Act (FOIA)*

2.2. *Government Records Access and Management Act (GRAMA).*

3.0 DEFINITIONS

4.0 POLICY

4.1 In compliance with federal law, UVU cannot guarantee privacy; neither shall a user have any expectation of privacy in any message, voice communication, file, image or data created, sent, retrieved, or received by use of the University's equipment and/or access. The University reserves the right to monitor any and all aspects of its computer systems and to do so at any time, without notice, and without the user's permission. The University holds as core values the principles of academic freedom and free expression. In consideration of these principles, the University shall not monitor the content of electronic communications of its employees in most instances, nor shall it examine the content of employee electronic communications or other employee electronic files stored on its systems except under certain circumstances. In this context, "electronic communications" include, but are not limited to, telephone communications, voice mail, e-mail, online chat, and computer files traversing the University network or stored on institution equipment. Examples of when monitoring and/or review may occur include, but are not limited to, the following circumstances:

1) Communications or files targeted by orders of a court of law or requested in accord with *GRAMA.*

2) Supervisor and/or Internal Audit review of university telephone system long-distance call records.

3) Electronic communications or files that have been inadvertently exposed to technical staff who are operating in good faith to resolve technical problems. When technical staff inadvertently see or hear potentially illegal content in communications or files, they are required to report what they have seen or heard to appropriate authorities. Otherwise, the University expects technical staff to treat inadvertently encountered electronic communications and files of university employees as confidential and not subject to disclosure to anyone.

4) Routine administrative functions, such as security tests of computing systems, including password testing by system administrators to identify guessable passwords, and investigations of attempted access into systems by unauthorized persons (system administrators and other technical staff shall not access employees' electronic communications or files while performing these functions).

5) Routine office functions.

6) Situations such as (a) an investigation into allegations of violations of law or policy, or (b) a reasonable or urgent need for access to university business documents when an employee is unavailable. Such situations shall be specifically reviewed by and approved by the president or the vice president (or equivalent) responsible for the affected employee(s).

7) For some units of the University, routine monitoring or examination of employee electronic communications or files as part of the work environment. Such routines must be approved by the relevant vice president (or equivalent), and affected employees must be informed in advance that such monitoring or examination shall be taking place.

4.2 This policy does not imply that the University has lower expectations for its employees' behavior. It expects university employees to obey all applicable policies and laws in the use of computing and communications technologies.

5.0 PROCEDURES

POLICY HISTORY		
Date of Last Action	Action Taken	Authorizing Entity