UVAW-15 - Appendix A - Guidance for Vice Chancellors on University of Virginia's College at Wise Policy on Monitoring/Review of Employee Electronic Communications or Files

Effective 10/12/05

Developed by the University of Virginia's College at Wise Office of Information Technologies
[Comments to s_herron@uvawise.edu]

Authority and Effective Date	Approved by the Chancellor – effective date is 10/12/05
Affects	All employees of the College
Subject/Purpose	Provides guidance for the Chancellor and/or Vice Chancellors who must consider and approve requests for authorization for non-law-enforcement College Information Technology personnel to monitor or review electronic communications or files of employees in conjunction with the Campus Police. This guidance is intended to accompany the UVAW – 15 University of Virginia's College at Wise Policy on Monitoring/Review of Employee Electronic Communications or Files.
Guidance text	**General** The College intends that authorization for non-law-enforcement College Information Technology personnel to monitor or review electronic communications or files of employees, including faculty and staff, will not be granted casually. Such authorization will require justification based on business needs or on sufficient cause from reasonably substantiated allegations of violation of law or policy on the part of the faculty or staff member. • Situations where there is an urgent need for access to College business documents when an employee is unavailable will require review and approval of the Vice Chancellor responsible for the affected employee(s) **or** the College Chancellor. • Situations where there is a need for an investigation into allegations of violations of law or policy will require review and approval of the Vice Chancellor responsible for the affected employee(s) **and** the College Chancellor. • for some units of the College, routine monitoring or examination of employee electronic communications or files as may be part of the work environment. Such routines must be approved by the relevant Vice Chancellor and the Chancellor, and all affected employees must be informed in advance that such monitoring or examination will be taking place.

Regarding investigations of violations of law or policy, in order to provide adequate checks and balances regarding requests for monitoring and/or review of electronic communications or files the request must have the authorization of a least two (2) parties for example:

- If the Vice Chancellor issues the request it must also be approved by the College.
- If the College Chancellor issues the request it must also be approved by the President of the University of Virginia.

Investigations of Violations of Law or Policy

Requests for authorization to monitor or review electronic communications or files because of allegations of violations of policy or law by faculty or staff members usually originate with supervisors. They may also originate with an investigatory authority such as the Director of Equal Opportunity Programs (looking into a sexual harassment claim, for example). A Vice Chancellor who is asked to consider authorization for monitoring or reviewing the electronic communications or files of an employee must use his or her judgment in determining if there is sufficient reason to grant such authorization. In these situations, the College expects the Vice Chancellor to maintain confidentiality and to consult with the Office of the General Counsel in determining whether to authorize monitoring or review and in determining if the affected employee or anyone else should be notified that the monitoring or review is taking place.

Business Needs

Examples of business needs include **but are not limited to**:

- the need to have access to the e-mail of an employee who is unexpectedly unavailable and who is conducting time-sensitive negotiations with an outside entity -- negotiations of sufficient importance to justify review of the employee's electronic communications and files when that employee is unable to give consent for that review
- an urgent and sufficiently serious issue of health or safety.

Often it will be desirable for the College to exercise diligence in enlisting the help of the employee to extract the business materials and in considering other steps to respect the personal nature of any other materials present if that help is unavailable. Such steps may include the use of an independent confidential reviewer -- a person on the College staff who does not have supervisory or management responsibilities for the employee whose materials are being reviewed -- to extract the business materials.

Circumstances Not Requiring Authorization

Most security tests of computing systems do not constitute monitoring or review of employee electronic communications or files. Consequently, Chancellor or Vice Chancellor authorization is not required for appropriate College staff to

	conduct such security testing, including testing done by system administrators to determine the strength of protection afforded by the passwords its employees select. In no case, of course, should employees reveal their passwords to anyone, including their system administrators. This testing is aimed at revealing weak or "guessable" passwords, and the appropriate action in responding to identification of a weak password is for the employee to change it immediately. Similarly, Chancellor or Vice Chancellor authorization is not required for appropriate College staff to review attempted access of its systems by persons (employees or others) not authorized to use them. Chancellor or Vice Chancellor authorization is also not required for review by appropriate College staff of records of the numbers employees call using the College's long-distance telephone system. Such reviews are routinely conducted as part of an Internal Audit review.