Information Technology / Computing Committee (ITCC) Report

to the MS&T Faculty Senate

February 21, 2008

At the February 21, 2008 Faculty Senate Meeting, the ITCC committee plans to make the following three motions:

1. The Faculty Senate requests that the Information Technology (IT) department create an official web page for each faculty and staff member. These pages should offer an optional link to individually-authored content, for which storage space should be provided.

2. The Faculty Senate recognizes that the oversight of the legality of web site content is the responsibility of the Administration. The Senate considers oversight of the appropriateness of web site content to be the responsibility of the Faculty, via the ITCC.

3. The Faculty Senate endorses the attached "M&ST Policy on Privacy in the Use of University Computing and Communications Systems". This policy was developed by the ITCC, with major portions adapted, or taken verbatim, from the March 2005 University of Missouri – Kansas City Policy by the same name]

MS&T Policy on Privacy in the Use of University Computing and Communications Systems

The Missouri University of Science and Technology affirms that fulfilling the academic mission of a university requires unfettered freedom of thought and expression. The University is a community dedicated to the life of the mind and to the free and open exchange of ideas. The teaching, research, service, learning and support activities conducted by faculty, students, administration and staff members require the use of communications and computing systems, which are owned by the University. We recognize that these activities are not possible without the expectation of privacy and confidentiality. Thus, we recognize the individual's right to privacy to the fullest extent possible under applicable laws.

The University community realizes that as more information is used in electronic form, serious concerns over possible unauthorized information access and invasion of privacy increase. This is particularly important in that assigned duties can often entail access to sensitive information. In particular, authorized Information Technology (IT) employees must be enabled to take timely actions to protect the integrity of computing and communications systems and comply with the law. The procedures and notifications involved in such access are delineated in the Designated Approving Authority section below, which is designed to delineate expectations of privacy by authorized users of computing and communications systems. It is also designed to protect the rights of these users and the University.

IT and other employees with access to private information must understand that using such access is explicitly prohibited unless it is unavoidable in the conduct of assigned duties. Furthermore,

employees are able to refuse requests for private information by referring the request to the Designated Approving Authority described below.

The following basic tenets will be adhered to:

- The University recognizes that all authorized users of university computing and communications equipment have a right of privacy in such use.
- Privacy, confidentiality, and freedom of thought and expression shall be paramount.
- The University will maintain a functional computing and communications system available to all authorized users and will protect and respect their privacy.
- Authorized users are defined as faculty, staff, students, and guest users with permission.
- Any release of private information shall be in accordance with the Designated Approving Authority section below.

Designated Approving Authority

Part 1. Computer and communications systems forensics required by law.

The University's IT organization will comply with legal requirements such as subpoenas, search warrants, and other actions compelled by law. Nothing in the University's policies shall be construed to circumvent this principle. The CIO, Provost, Chancellor, and Faculty Senate President shall be informed of such activities if informing them is permitted by law. Authorized users of affected systems will also be informed if permitted by law.

Part 2. All other forensic investigations.

To ensure privacy of network communications and computer usage, all campus forensic investigations which are not break/fix or network stability issues must be authorized by the appropriate Designated Approving Authority (DAA) as indicated below. The authorization will also define the scope of the investigation and time limit for the investigation to be conducted.

Investigations of operational issues (break/fix) or network stability issues are part of the day-to-day operations of the office of Information Systems Security and are allowed to be conducted without being authorized. To clarify exactly what this means, personnel are allowed to conduct investigations in the cases where:

- Network anomalies are occurring and threaten the stability of the network
- Intrusion Detection system operation with very limited rules to indicate threats to the campus network.
- Network/systems vulnerability checking
- University owned equipment involved in above situations, personnel will attempt to contact primary user of the system first, but if they are not available, security personnel are allowed to examine the system for the exact cause of the anomaly to stop the problem.
- Personally owned systems are examined only with owner permission.

Any information accidentally encountered during these scenarios will be ignored, with the exception of violations of law, such as child pornography. If such violations are encountered, the matter will be promptly turned over to the appropriate governing body for their review.

All personnel in the office of Information Systems Security must abide by this policy and any violations of this policy by IT staff will be reviewed by the Chief Information Officer and HR Director for possible sanctions.

Scope
This policy applies to personnel trained and authorized to perform network and computer forensics services.

Authorized Approving Individuals
The Designated Approving Authority for the University of Missouri – Rolla Campus can be one or more of the following and the groups they are limited to authorize a request for are:

Authorized Approving Authority	Limited To
Faculty committee: One designee of Chancellor or Provost; One department Chair, Three faculty members selected by Faculty Senate.	faculty
One Designee of the Human Resource Director, Two staff members selected by Staff Council Two faculty members from the group listed above	staff
One designee of the Vice Chancellor of Student Affairs, Two student members selected by the Student Government Two faculty members from the group listed above	students

Collection Rule
As information stored on systems or storage media can be very time critical, any of the above may also issue a data collection only approval, and later issue a forensics authorization. Also, in cases where time is critical and the above Designated Approving Authorities are unavailable, the Chief Information Officer (CIO) or designee may authorize a request to collect material only with no possible forensics being conducted until the proper DAA is available. The CIO or designee must also notify the appropriate primary approving authority of the collection. Also in this case, if the Chief Information Officer elects to use a designee, the designee cannot be any person(s) directly involved with the forensic process. Under this situation, formal approval will be solicited from the appropriate primary approving authority at the earliest feasible time.

Exceptions to the Collections Rule:

No DAA requirement is required for doing full disk image backup and email backup with non-friendly termination. This is part of the standard procedure to ensure as much data is retained in case of litigations with a non-friendly termination and is for liability protection of the University. Any forensics conducted on these backups will require a DAA authorization before the forensics may be initiated. All such backups must be destroyed after 12 months if no litigation appears to be imminent.

Scope of Request
The scope of the forensic items covered by this authorization is:

- The scope of the information requested needs to be specified at the time it is made – no open ended requests are allowed.
- Full network packet capture and analysis of an individual system(s)

- Forensics investigation of a University owned system or a group of systems and/or storage media, such as hard drives, USB memory device, CD, etc. Only a Law Enforcement request may be issued for a personally owned system or storage media.

- Forensic analysis of network storage such as email or the University supplied network file storage system.

- A time period not to exceed 30 calendar days per authorization.

Appeal
If possible in the context of any approved forensic collection, authorized users may appeal the decision of the Authorized Approving Authority above to the following bodies:

Appeal to	Limited To
Chancellor or Provost; Rules, Procedures and Agenda Committee of Faculty Senate.	faculty
Human Resource Director, Staff Council	staff
Vice Chancellor of Student Affairs, President and Vice President of Student Government	students

References:

None.