Procedure for Monitoring of IT Resources

The University may monitor FSU IT resources and retrieve communications and other records of specific users of FSU IT resources, including individual login session and the content of individual communications, without notice. The criteria and steps required for approval of such monitoring or retrieval without notice are set forth in this policy.

A request for such monitoring or retrieval of records and documents must be provided to the FSU's Legal Counsel with the appropriate Vice Chancellors' approval and detailed justification for the request. If the records are being monitored or retrieved for the purposes of reviewing or investigating employee conduct, the approval of the Associate Vice Chancellor for Human Resource is also required.

Prior approval is not required to monitor FSU IT resources or retrieve communications and other records in the following situations:

- The communications and/or records have been made accessible to the public, as by posting to a webpage.
- A person's authorization to access or use any FSU IT resources ends, for example upon termination of FSU employment or appointment.
- The monitoring or retrieval is in response to an emergency. An emergency occurs when there is an imminent threat to life or property and there is not sufficient time available to obtain approval. In such a situation, monitoring or retrieval may be conducted without prior approval, with notification to the appropriate Vice Chancellor and the General Counsel as soon as possible. The scope of access should be reasonable in relation to the emergency situation involved.
- The monitoring or retrieval is required to respond to external regulatory agencies that detected violations or abuse over the Internet by FSU constituents.

Approval may be granted to monitor communications or retrieve records when any one or more of the following situations apply:

- It reasonably appears necessary or appropriate to do so to protect the integrity, security or functionality of university or other computing resources.
- It reasonably appears necessary or appropriate to do so to comply with legal or contractual requirements or to protect the university from liability or disruption. Examples of situations in which access and retrieval are authorized under this paragraph include but are not limited to responses to public records requests, subpoenas, court orders, and discovery requests,
- There is reasonable cause to believe that the user has violated or is violating the Acceptable Use Policy or that the user has violated, or is violating, any other university or Board of Governors rule, regulation, policy, or collective bargaining agreement, or any other law or regulation and the access is reasonable in relation to the believed violation.
- It is part of any investigation or review of an already asserted, threatened or potential complaint or grievance or of a credible allegation of a violation of the law, including without limitation local, state or federal law, or foreign law as applicable, or university or Board of Governors rule, regulation or policy, or the

subject of a law enforcement review or investigation, and the scope of access to the account or activity is reasonable in relation to the complaint, grievance or allegation.

- An account appears to be engaged in unusual or unusually excessive activity.
- The University has a legitimate need to access an account or activity and the access is reasonable in relation to the need.

The results of any such general or individual monitoring, including but not limited to the contents and records of individual communications, may be released pursuant to a public records request. In addition, the university, in its discretion, may disclose the results of any such general or individual monitoring for any legitimate purpose to appropriate university personnel or law enforcement agencies and may use those results in appropriate external and internal disciplinary and other proceedings