Purpose:

The purpose of this policy is to define how The University may monitor UF Information Technology (IT) resources and retrieve communications and other records of specific users of UF IT resources.

Scope:

This policy covers monitoring and retrieval of all forms of electronic communications and data stored or transmitted on University Information Systems, including individual login sessions, stored files and the content of individual communications.

Policy:

1. Approval must be obtained and provided to the Vice President and Chief Information Officer prior to monitoring or retrieval of IT resources, except as specified within this policy. Approval must be obtained from the appropriate senior leadership:
   a. Vice President and General Counsel (or designee) in all situations.
   b. Vice President for Human Resources (or designee) when the university is reviewing or investigating employee conduct.
   c. Vice President for Student Affairs (or designee) when the university is reviewing or investigating student conduct.

2. Approval may be granted to monitor or retrieve IT Resources when any one or more of the following situations apply:
   a. It reasonably appears necessary or appropriate to do so to protect the university from liability or disruption.
   b. 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.
Policy: Monitoring of IT Resources

c. 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.
d. The University has a legitimate need to access an account or activity and the access is reasonable in relation to the need.

3. No prior approval is required to monitor UF IT resources or retrieve communications and other records in the following situations:

   a. When needed to comply with legal or contractual requirements, e.g. public records requests or subpoenas.
   b. The communications and/or records have been made accessible to the public, as by posting to a webpage.
   c. A person’s authorization to access or use any UFIT resources ends, for example upon termination of UF employment or appointment.
   d. 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 Vice President and Chief Information Officer and the General Counsel as soon as possible. The scope of access should be reasonable in relation to the emergency situation involved.
   e. Monitoring or retrieval for the purposes of detecting or investigating a computer security incident or Data Breach. Approval must be obtained to release communications and/or records gathered as part of an investigation to persons other than members of the Computer Security Incident Response Team or Privacy investigation team.
   f. It reasonably appears necessary or appropriate to do so to protect the integrity, security or functionality of university or other computing resources.

Responsibilities:

1. The Vice President and Chief Information Officer is responsible for verifying that appropriate approvals are obtained when required.
Policy: Monitoring of IT Resources

Authority:

UF-1.0102: Policies on Information Technology and Security

References: