Columbus State University
Data Privacy Policy

Created 1/22/2018

1.0 Background
All USG institutions, the University System Office (USO), the Georgia Public Library System (GPLS), and the Georgia Archives must comply with the information security and privacy policies, standards, and procedures issued by USG Cyber Security, and report and file the appropriate compliance documents as identified in this policy. All USG institutions, the USO, the GPLS, and the Georgia Archives must adhere to the Information Security Reporting Requirements, as noted in Section 5.10 of the USG IT Handbook. (see footnote 1)

2.0 Purpose
The Columbus State University (CSU) Data Privacy Policy provides the standards the University follows when accessing the files and communications of its students and employees. In the interest of promoting academic freedom and the mission of the University, CSU recognizes its obligation not to infringe upon the reasonable privacy expectations of its employees and students in their electronic communications and data.

3.0 Policy
CSU provides information technology resources to faculty members, staff and students for the purpose of furthering CSU's mission and conducting CSU business. While personal use of such systems is permitted, as per the CSU Appropriate Information Systems Use policy, personal communications and files transmitted over or stored on CSU systems are subject to the same regulations as business communications.

CSU is committed to respecting the privacy expectations of its employees and students. Consistent with this policy, electronic information that is transmitted over or stored in CSU systems and networks is subject to being audited, inspected and disclosed to fulfill administrative or legal obligations which may include, but are not limited to, the following:

- Is necessary to comply with legal requirements or process (e.g., Georgia Open Records Act or subpoena).
- May yield information necessary for the investigation of a suspected violation of law or regulations, or of a suspected infraction of CSU or Board of Regents policy.
- Is needed to maintain the security of CSU computing systems and networks.
- Is needed for system administrators to diagnose and correct problems with system software or hardware.
- May yield information needed to deal with an emergency; is needed for the ordinary business of the University to proceed, (e.g., access to data associated with an employee who has been terminated/separated or is pending termination/separation, is deceased, is on extended sick leave, or is otherwise unavailable).
- Is necessary to comply with a written request from the Vice President of Student Affairs on behalf of the parents, guardian, or personal representative of the estate of a deceased student.
- Is for research authorized by CSU under a data use agreement that precludes the disclosure of personally identifiable information.

4.0 Procedures & Responsibilities

Where possible, all CSU applications and systems must display the following login banner to all users prior to authentication of user credentials:

> **TERMS OF USE**
> This information technology resource is the property of the Columbus State University and is available for authorized use only, in accordance with the University System of Georgia (USG) and CSU UITS policies (https://infosec.columbusstate.edu/securitypolicies/security_policies.php). Any and all files on this system are subject to being audited, inspected and disclosed to authorized system administrators and/or law enforcement personnel to fulfill administrative and/or legal obligations. By using this system, you acknowledge and agree to these terms.

All internal requests for access to information that is transmitted over or stored on CSU systems and networks should be directed to the Chief Information Officer or designee. The determination of whether access to information is necessary to fulfill administrative is made by the Chief Information Officer or designee, and may not be made at the departmental or unit level.

This policy governs access to the files and communications transmitted on or stored in CSU IT Resources.

Any individual whose personal files and communications exist on a CSU IT Resource by virtue of unauthorized access will have no expectation of privacy.

If you become aware of any non-compliance of this CSU Privacy Policy inform **InfoSec (abuse@columbusstate.edu) or** the UITS Help Desk **(helpdesk@columbusstate.edu)** immediately.

Footnote:

(1) http://www.usg.edu/information_technology_services/it_handbook/