Georgia Institute of **Tech**nology

Data Privacy Procedures

Effective Date: December 2016
Last Revised: June 2017

Procedure Owner: Georgia Tech Cyber Security
Procedure Contact: Information Security Standard and Compliance Manager

1. Reason for Procedure

The Data Privacy Procedures support the Data Privacy Policy.

2. Scope

This procedure governs access to the files and communications transmitted on or stored in Georgia Tech's IT Resources.

3. Procedures

Business Continuity

Access may be provided without prior consent where it is determined, in consultation with the Office of Human Resources, that the information is needed for the ordinary business of the Institute 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).

Please see business continuity requests link in the related information section.

Deceased Students

Information will be accessed in response to a written request from the Vice President for Student Life on behalf of the parents, guardian, or personal representative of the estate of a deceased student.

Emergency

Access may be provided without consent where necessary to address an emergency situation. If feasible, such requests will be granted in consultation with the Office of Student Life, for student information, or with the Office of Human Resources, for faculty or staff information.

Legal Requirements
Information will be accessed as necessary to comply with legal requirements, including responses to subpoenas for the production of documents and requests for inspection and copying of documents under the Georgia Open Records Act.

Research
Access may be provided without consent for research authorized by Georgia Tech under a data use agreement that precludes the disclosure of personally identifiable information.

System Integrity
Access may be provided without consent where needed for system administrators to diagnose and correct problems with system software or hardware or to maintain the security of Georgia Tech computing systems and networks.

Violation of Law or Policy
Access may be provided without notice or consent when it is determined by the Office of Legal Affairs and Risk Management that such access may yield information necessary for the investigation of a suspected violation of law or regulations, or of a suspected infraction of Georgia Tech or Board of Regents policy.

Other Conditions
For conditions other than those covered above, access may be granted where deemed necessary by the consensus of the Office of Legal Affairs and Risk Management, the Chief Information Security Officer, and the Office of Human Resources (for employee-related issues), or the Dean of Students (for student-related issues).

4. Related Information

Resource	Link
Business continuity requests	https://security.gatech.edu/business-continuity-requests
Data Privacy Policy	https://policylibrary.gatech.edu/information-technology/data-privacy-policy

5. Procedure History

Revision Number	Author	Description
1.0	Cyber Security	Initial release
1.1	Cyber Security	Minor additions
1.2	Cyber Security	Minor additions
1.3	Cyber Security	Added link to business continuity requests