Data Access Procedures

Rev. 1.9.6

Effective Date: November 2, 2005
Last Review Date: July, 2015

Directly in support of the following Policy Document(s):
Georgia Institute of Technology Data Access Policy

The following are responsible for the accuracy of the information contained in this document

Responsible University Officer

Associate Vice President / Associate Vice Provost for Information Technology and Chief Information Officer (CIO)

Responsible Coordinating Office

Office of Information Technology (OIT)

1. Executive Summary

This document is in direct support of the *Georgia Institute of Technology Data Access Policy* and is included by reference in the policy. This document sets forth guidelines and procedures for requesting access to *Institute Data*, and in particular to *Sensitive Data* as defined in the Data Access Policy. This document shall be subject to periodic changes and updates, as necessary, independent of the policy document itself.

(**NOTE**: Phrases shown in *italics* at their first occurrence in this document are defined in the associated IT Policy Definitions - Standards Document No. 05.GIT.170)

2. Procedures

a. *Data Coordinators* assist with data classification. Data Coordinators grant access to the data within their purview according to criteria defined for specific access requirements. For example, some types of access require training, the establishment of user accounts, and awareness of federal or State guidelines restricting data access.

b. *Authorized Requesters* represent a campus unit or group of campus units, and are appointed by someone with at least unit head authority. Every organization determines the best way to assign this responsibility based upon workflow, organizational structure, and job responsibilities.

c. Authorized Requesters verify individual access requirements, and forward access requests to the appropriate Data Coordinator. Authorized Requesters assure that access

privileges are kept current with changes in personnel status for individuals in the unit(s) represented.

d. Data Coordinators will provide assistance as required to Authorized Requesters to assure that access privileges are granted in accordance with the Policy.

e. The requests are initiated via email or applicable web form, and forwarded to the appropriate Data Coordinator. If the request requires electronic access to data, it is then forwarded to the appropriate *Data Administrator* for action.

f. Access requests should include the following information:
   - Department Name
   - User Name
   - User ID (if one has already been assigned)
   - Job Title
   - Phone Number
   - What Data/Role & Why (Data Coordinators will provide assistance)
   - Access End Date (some individuals only require temporary access)
   - All expected user groups for the data requested (i.e. will the data be released to third parties?)

   Note: Any change or extension to the original intended use of the data requested (as documented in the original access request), such as a new application being developed using data for which access was previously granted, shall require a new access request explicitly documenting such change or extension.

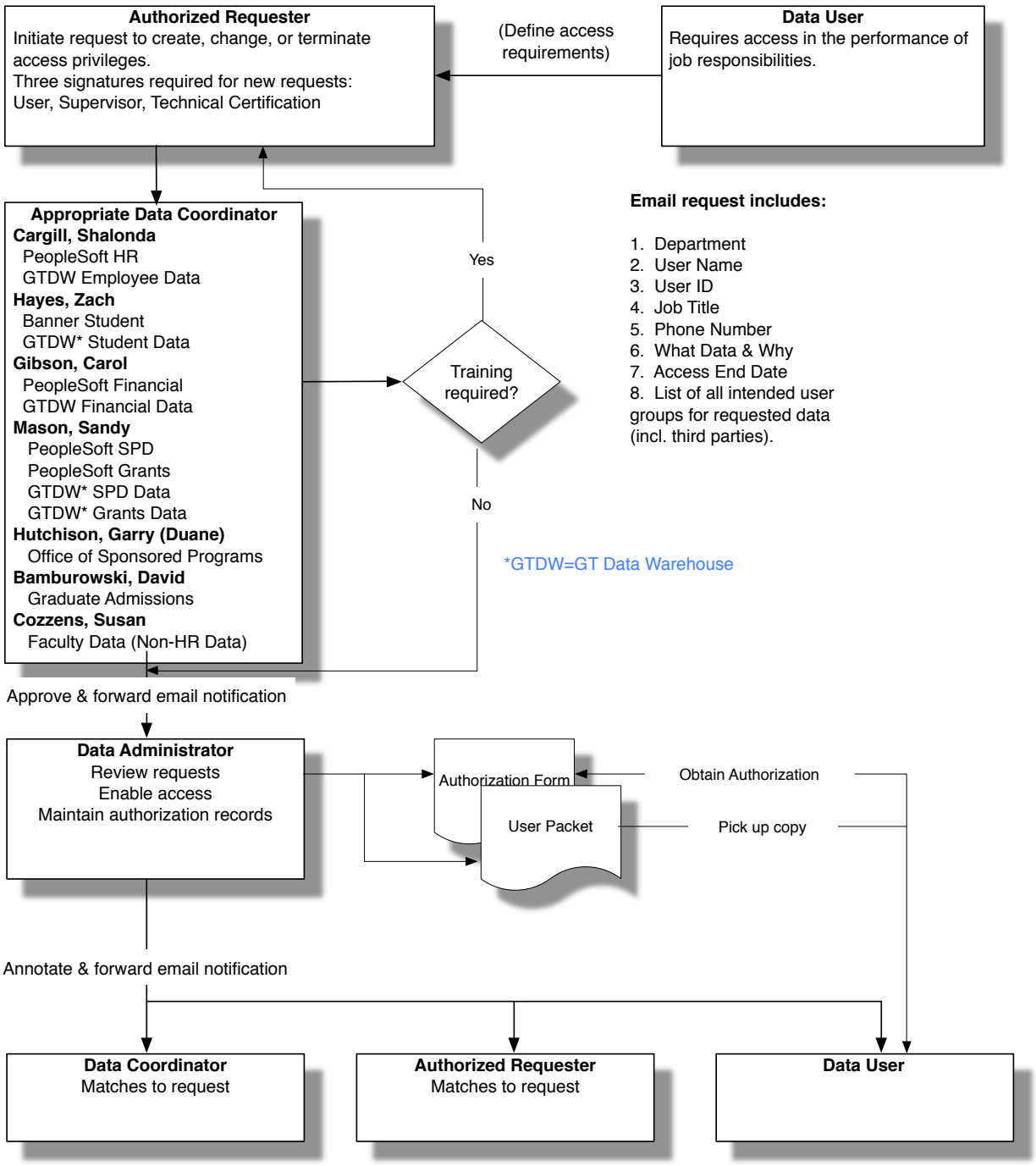
g. All data access requests must have a minimum of three certifications: i) *Data User*: acknowledging having received the Institute's Data Access Policy; ii) Supervisor/Departmental Certification: authorizing data user to access data based on job responsibilities, and verifying the accuracy of the information conveyed on the data access request form; and iii) Technical Certification: approval of the corresponding *Technical Authority* for the data user's department, certifying the technical compliance of the client and/or server machines to be used by the data user to access the information. Additional certifications may be required by individual department policies and/or systems.

h. If an individual is requesting access to data that has associated prerequisites, such as Banner and PeopleSoft training, or review of Family Education Rights and Privacy Act (FERPA) and/or Gramm-Leach-Bliley Act (GLBA) Sensitive Data Access guidelines, then the Data Coordinator will ensure that the prerequisites have been met prior to approval.

i. Data Coordinators and Data Administrators will maintain electronic archives of all requests. Data Administrators will serve as the point of contact for related audit reviews.

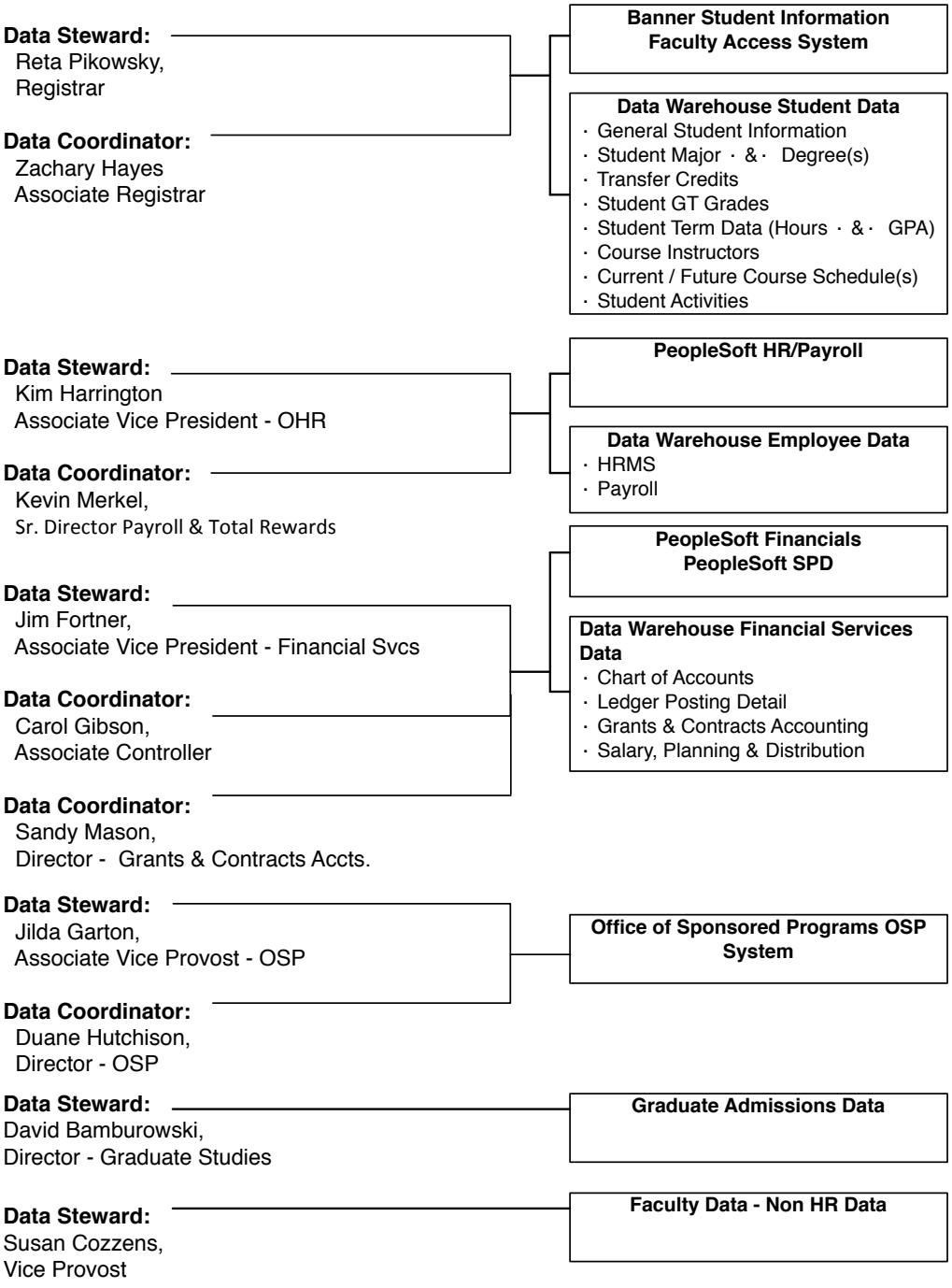
j. Data Administrators will maintain a repository of information regarding the data classified by the *Data Stewards* and Coordinators.

Procedure for Requesting Data Access to Institute-wide Systems
(as of February 2015)



Chief Stewards, Data Stewards, and Primary Data Coordinators for Institute-wide Systems

(as of July 2015)



3. Revision History

Revision Number	Author	Description
1.9.6	Jimmy Lummis	Updated Data Stewards and Coordinators
1.9.5	Jimmy Lummis	Updated Data Stewards and Coordinators
1.9.4	Jimmy Lummis	Updated Data Access Request diagram
1.9.3	Herb Baines	Updated Data Stewards diagram
1.9.2	Richard Biever	Updated Data Coordinator contact information
1.9.1	Richard Biever	Updated Data Coordinator contact information.