AUBURN UNIVERSITY
STUDENT AFFAIRS

Assessment & Strategic Planning
POLICIES ON CONFIDENTIALITY OF DATA

Student Affairs Assessment & Strategic Planning (A&SP) regards the confidentiality of data and information to be of utmost importance. Therefore, A&SP requires all Student Affairs employees and users of data to adhere to the *ACPA/NASPA Professional Competencies* and the ACPA ASK Standards, in particular the competencies pertaining to data security and ethics, and requires all users of data and information to follow the procedures outlined below.

Policy on Confidentiality of Data

Each employee, consultant, student, or person granted access to data and information holds a position of trust and must preserve the security and confidentiality of the information they use. Users of University data and information are required to abide by all applicable Federal and state guidelines and University policies regarding confidentiality of data, including, but not limited to the Family Education Rights and Privacy Act (FERPA) and the Health Insurance Portability and Accountability Act (HIPAA). All A&SP employees must read and understand how the FERPA policy applies to their respective job functions.

Any A&SP employee, university employee, or authorized person/s with access to Auburn University's computer resources, information system, records, or files is given access solely for the business of the University. Specifically, individuals should:

a) Access data solely in order to perform their job responsibilities.
b) Not seek personal benefit or permit others to benefit personally from any data that has come to them through their work assignments.
c) Not make or permit unauthorized use of any information in the University's information system or records, including the release of directory information.
d) Not enter, change, delete or add data to any information system or files outside the scope of their job responsibilities.
e) Not include or cause to be included in any record or report, a false, inaccurate or misleading entry.
f) Not alter or delete or cause to be altered or deleted from any record, report or information system a true and correct entry.
g) Not release University data other than what is required in completion of job responsibilities.
h) Not exhibit or divulge the contents of any record, file, or information to any person, except as it is related to the completion of their job responsibilities.
i) Take measures to ensure that their workstation, confidential documents, and office keys are not accessible to unauthorized individuals.

j) Regularly check for and install or have installed appropriate operating system and application software patches to protect their assigned computer (or any other computer that is used to complete job responsibilities) from known vulnerabilities.
k) Maintain the strict confidentiality of all confidential information accessed during employment or affiliation and into the future after any termination of employment or affiliation, without limit.
l) Only store data in locations approved according to the classifications in the Auburn University Data Storage Matrix.

Additionally, individuals are not permitted to operate or request others to operate any University data equipment for a personal business venture, to make unauthorized copies of University software or related documentation, or to use such equipment for any reason not specifically required by their job responsibilities.

Policy on Disposal of Confidential Information/Data

Confidential information or data may be located on various media including, but not limited to, secure electronic file shares, encrypted USB drives, paper documents, diskettes, hard drives, tapes, and compact disks (CD/DVD). Confidential information shall not be discarded in trash bins, placed in unsecured recycle/burn boxes, or left in areas accessible to the public or to persons not authorized to access the information. Disposal of media containing any confidential information shall be according to the following methods:

a) Confidential information on paper media (including all those with social security numbers) shall be disposed of using a proper paper shredder (see A&SP staff member), or placed in a designated recycle/burn box, if available, for approved external destruction.
b) Diskettes or hard-drives that will be transferred outside of SA A&SP shall be sanitized according to the United State Department of Defense standard 5220.22-M or a more stringent methodology. Alternatively, these media may be physically destroyed to prevent unauthorized access to the data on the media.
c) Other media, including but not limited to, CD/DVD shall either be physically destroyed or otherwise sanitized to prevent unauthorized access to the data on the media.

It is the responsibility of the data user to report immediately to their supervisor any violation of these policies or any other action that violates the confidentiality of data.

The above documented policies on Confidentiality of Data from Student Affairs Assessment & Strategic Planning are in addition to the Auburn University *Information Disclosure and Confidentiality Policy* and *all AU Information Technology policies.* Employees and data users are expected to adhere to all Student Affairs guidelines and procedures and all Auburn University policies.

AUBURN UNIVERSITY
STUDENT AFFAIRS

ASSESSMENT & STRATEGIC PLANNING
Policies on Confidentiality of Data

I understand that my access to University data and information systems is for the sole purpose of carrying out my job responsibilities. I recognize that breach of confidentiality, including aiding, abetting, or acting in conspiracy with any person to violate any part of this policy, may result in sanctions, civil or criminal prosecution and penalties, employment and/or University disciplinary action, and could lead to dismissal, suspension and/or revocation of all access privileges.

I have read the above policy and agree to comply with Student Affairs Assessment & Strategic Planning Policies on Confidentiality of Data, and any updates or revisions published and distributed.

Employee/Data User's Name (Please Print)

Employee/ Data User's Signature

Date

Policy Revision Date: 05/05/2021