AUBURN UNIVERSITY
Office of the Registrar

AUBURN UNIVERSITY

POLICY ON CONFIDENTIALITY OF DATA

The Office of the Registrar (OTR) regards the confidentiality of data and information to be of utmost importance. Therefore, the OTR requires all users of data and information to follow the procedures outlined below in addition to applicable law and University policy:

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 he/she uses. 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 University's Information Disclosure and Confidentiality Policy, Appropriate Use of Information Technology Policy, and Data Access Policy. All University employees using University data must read and understand how these policies apply to their respective job functions.

Any authorized access granted to Auburn University's computer resources, information system, data, records or files must be used solely for legitimate University business reasons or to carry out the user's official duties. Specifically, individuals should:

a. Access data solely in order to perform his/her 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 or transmission 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 or any record, file or information system 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.

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. Employees may use their assigned office equipment and application software, including

E-mail and instant messaging, for personal or educational pursuits, as long as no portion of this policy or other applicable University policy or law is violated by doing so.

Confidential information or data may be located on various media including, but not limited to, 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 done in accordance with the University's Electronic Data Disposal Policy (https://sites.auburn.edu/admin/universitypolicies/Policies/ElectronicDataDisposalPolicy.pdf).

It is the employee's responsibility to report immediately to his/her supervisor any violation of these policies or any other action that violates the confidentiality of data.

Revision Date: 09/18/2023