SAINT AUGUSTINE'S UNIVERSITY
Data Confidentiality Agreement Policy

Employees' first and primary obligation is to carry out their workplace responsibilities professionally, objectively, and ethically in a manner that is consistent with the best interest of Saint Augustine's University. The divisions of Institutional Research & Information Technology at Saint Augustine's University are the owners of all institutional data available in all types of university electronic systems. An individual's access to university data is granted on a need-to-know basis and as required to perform job duties and functions related to the current institution of employment.

Access to institutional data is approved by the Institutional Research Staff, an individual who has direct responsibility to ensure that a data domain is classified appropriately. Every individual or entity with access to SAU Institutional Data has an obligation to use and secure institutional data, which includes student, employee, financial, and medical information; appropriately. Each data user will be granted access to the Institutional data only after carefully reading the Data Confidentiality Agreement (DCA) policy followed by signing the DCA DocuSign. Please allow three business days for granting access after submitting the DocuSign.

Individuals and entities with access to institutional data must agree to:

- Respect electronic computing resources and systems and my impact on them.
- Utilize information available for my use in my official role at SAU only. No additional uses of information or sharing of information may be made without appropriate authorization.
- Removal of official record copies of documents from the office where they are maintained is permissible only when authorized to do so and in the performance of office duties.
- Keep all passwords and access codes confidential and out of sight of others.
- Keep all confidential (high-risk) information and records however maintained or stored, safeguarded against inappropriate use or access by others. Physical documents must not be left unattended and must be securely stored in locked storage.
- Never store confidential (high-risk) information in any format on a thumb drive. All devices that access high-risk data must be managed in an institution or SAU system-approved manner (even though your SAU Google Drive account is an institutional-approved storage solution, it is not appropriate for high-risk data. Please use a Network Drive instead). The system must be locked and logged out when unattended.
- When accessing confidential (high-risk) data, encryption needs to be applied at rest and in transit.

- Report any infractions in the use or release of information to the appropriate data steward.
- Destroy stored institutional data securely.
- Remove SAU System data from their personally owned devices before the devices are discarded or replaced, or before the individual is no longer employed with the SAU, unless explicitly authorized to retain the data.

Users who fail to adhere to the provisions of this policy may result in the suspension or loss of access to SAU System IT resources; appropriate disciplinary action as provided under existing procedures applicable to students, faculty, and staff; civil action; or criminal prosecution. To preserve and protect the integrity of SAU System IT resources, there may be circumstances where a SAU may immediately suspend or deny access to the resources.

Note: High Risk – Any data where the unauthorized disclosure, alteration, loss, or destruction may
cause personal or institutional financial loss or the unauthorized release of which would be a violation of a statute, act, or law.

ACKNOWLEDGEMENT

I have read the SAU Data Confidentiality Agreement Policy. I understand my responsibilities and obligations regarding data security and confidentiality.

First Name: _____ Last Name: _____

Signature: _____ Date: _____

Please submit a scanned copy of this agreement form to Institutional Research Staff (Dr. Indrani Singh) after entering all details and adding the handwritten signature in the acknowledgement.