Procedure Name	Clemson University Advancement - Data Use Procedure		
Procedure #	**6.1**	**Effective Date**	February 20, 2026
Responsible Department	CUF IT	**Cross Reference**	6.1
Policy Approved by	Data Governance Executive Council, CUF Senior Staff	**Procedure Owner:**	Executive Director of IT

1. Access

Granting, Updating, and Removing Access

- **Advancement Employees**
  - Access will be role-based and aligned with job responsibilities.
  - Supervisors should follow their department's onboarding procedure, which includes a request to grant CADENCE access.
  - New employees will be required to affirm the Data Use Policy and complete training before access is provided.
  - Supervisors should off-board employees using their department's process which includes a request to remove CADENCE access on termination date.
- **University Partners (University employees or volunteers outside Advancement)**
  - Access and removal requests must be submitted by a sponsoring Advancement Data Access Manager.
  - Approval requires confirmation that data is necessary for job duties directly supporting Advancement's mission.
  - Data Consumer will be required to affirm Data Use Policy before access is provided.

a. **Auxiliary Users**

- Self-serve access to CADENCE is divided into Auxiliary with or without Revenue based on function.
- Only a limited number of user accounts have been approved for Data Consumers outside of the Division. Requests for additional Auxiliary Users will be reviewed and managed by the Data Governance Council. Existing list is below:

University/Auxiliary Department	Pre-approved Position	Assigned Access Manager
President's Office	Executive Assistant to the President, Chief of Staff, Asst to the Chief of Staff, Project Manager	Presidential Engagement Coordinator
Provost Office		Presidential Engagement Coordinator
Financial Aid	Director of Scholarships, Scholarship Coordinator	Director of Donor Relations

Internal Audit	Auditor	Director of Gift and Records Management
Clemson World	TBD	Director of Gift and Records Management
Supporting University Affiliates per SLAs (e.g. IPTAY and Clemson Architectural Foundation)	Per Service Level Agreement (SLA)	Clemson University Foundation Legal Counsel

b. Non-Auxiliary Users

- A larger group that receives data generated and/or published by Advancement staff (e.g. business officers and stewardship liaisons in the colleges/units).
- These Data Consumers do not have direct access to CADENCE; however, they are required to review, export, and/or share data using only University-approved applications and processes.
- SharePoint Secure – is the recommended application for sharing data to Data Consumers.
- IT Team will set up access to SharePoint Secure. Data Access Manager will be able to add, update, and delete files per individual Data Consumer.

3. Volunteers

- Access and removal requests must be submitted by a sponsoring Advancement Data Access Manager.
- Approval requires confirmation that data is necessary for Volunteer duties directly supporting Advancement's mission. (e.g. Class Reunion Chair, Campaign Cabinet Member). These Data Consumers do not have direct access to CADENCE.
- Data Consumer will be required to affirm Data Use Policy before access is provided.
- IT Team will set up access to SharePoint Secure. Data Access Manager will be able to add, update, and delete files per individual Data Consumer.
- Learn more about securing data:
    - Clemson University Cybersecurity Recommendations
    - Clemson University Cybersecurity Training (online)
    - Clemson University Email Best Practices
    - Clemson University Email Encryption Tutorial

4. Vendors

- Vendor access requests must follow the Clemson University Foundation Vendor Management Policy.
- Vendors must sign a non-disclosure agreement (NDA) prior to receiving data.
- Vendor's Data Access Managers are responsible for documenting specific business use and related contract terms.

- These Data Consumers do not have direct access to CADENCE; however, they are required to review, export, and/or share data using only IT and University-approved applications and processes.
- IT Team will set up access to SharePoint Secure. Data Access Manager will be able to add, update, and delete files per individual Data Consumer.
- Learn more about:
    - Clemson University Vendor Management Policy
    - Advancement's Vendor Management Procedure

Data Access Manager Responsibility:

- Data Access Managers are responsible for ensuring the accuracy of Data Consumers under their purview and promptly alerting changes to CUF IT.
- Data Access Managers should communicate with their assigned Data Consumer(s) at least quarterly.
- Data Access Managers are responsible for the knowledge/training, and enforcement of proper usage of information.
- Data Access Managers are responsible for notifying Advancement Services IT immediately when a Data Consumer's role changes or employment/volunteer relationship ends.

2. Data Retention and Disposal

- Data previously stored locally by the User must be securely deleted or returned to CUF IT.
- Users must follow Clemson University Data Retention and Disposal
- Disposal must be performed through secure shredding, deletion, or other approved methods.
- CUF IT will purge processing files as described in their Retention Schedule.

3. Compliance and Enforcement

- Data Use Policy and Procedures will be reviewed annually.
    - CUF Senior Staff, Data Governance Council Executive Committee, and CCIT will review any changes to verbiage, legal obligations, etc.
    - IT Team will review the data accessed, timeframe, and disposal.
- All Data Consumers will be required to reaffirm updated Data Use and/or other relevant policies.
    - A data audit will be conducted to review compliance and effectiveness.
- Data Incidence/Breach
    - Clemson University Information Security Incident Reporting Procedures
    - Clemson University Advancement Data Breach Response Plan Policy
- Supervisors and/or Data Access Managers will be notified of non-compliance.