Procedure No.	B600.00.40.01.D
Policy No.	
Date	September 2003
Revised	December 2012
Revised	August 2017
Revised	September 2017

COLLEAGUE ACCEPTABLE USE PROCEDURE

PURPOSE

Rowan-Cabarrus Community College (RCCC) provides its employees access to administrative data as required for the performance and fulfillment of job responsibilities. The access is provided for administrative purposes that support the college's mission. Access must be reviewed semi-annually and signed annually.

POLICY

The use of administrative data is a privilege, not a right. Inappropriate use reduces the availability of administrative data for critical operations, compromises college security and network integrity, and leaves the college open to potential litigation; therefore, inappropriate use may result in the cancellation of this privilege. Users are subject to the requirements for authorization, notification, and other conditions specified in this procedure and related procedures. The college may inspect, monitor, or disclose administrative data transactions when required by and constituted by law and/or when there is substantiated reason to believe that violations of any federal, state, or local law or any violation of Rowan-Cabarrus Community College's policies or procedures have taken place.

PROCEDURES

1. User Responsibilities

   RCCC faculty and staff are authorized users of the college's administrative data upon approval of the appropriate Data Administrator/Custodian. **It is the responsibility of authorized users to use administrative data in a manner that maintains the confidentiality and security of administrative data.** Users are authorized to access only the specific administrative data outlined in the signed CIS User Access Form.

   a. Authorized users shall not use RCCC's administrative data access to dispense administrative data to unauthorized college employees, to external personnel, or organizations without authorization.

   b. Authorized users are required to terminate administrative data sessions when the computer is not manned by the authorized user. An authorized screensaver requiring a password on resume must be maintained and active on all college computers with CIS access.

c. Authorized users are responsible to avoid the spread of computer viruses. Personnel shall not download or install unauthorized software (software not owned or registered to the college).

2. Staff Responsibilities

a. It is the responsibility of Data Administrators to initiate new access, or Data Administrators/Custodians to change access to specific administrative data for employees by completing the CIS User Action Form (form 1.27 A); review this procedure and the agreement with each employee; have the employee sign the agreement; and forward the signed and approved agreement to ITS.

b. It is the responsibility of the Data Administrator to authorize security class creations and Data Administrators/Custodians to authorize modifications. All security class changes will be signed by the appropriate Data Administrators and submitted to ITS. (Form 1.27 C).

c. It is the responsibility of Data Administrators/Custodians to **semi-annually** review access to specific administrative data for employees by signing the CIS Security listing provided semi-annually by ITS; review the access listed with each employee. The signed and approved review is then submitted to ITS (form 1.27 D).

d. It is the responsibility of designated CIS Data Administrator/Custodian or designated trainer to conduct local CIS administrative data training for new CIS users. Training classes are also available via the North Carolina Community College System Office per their training schedule. Following training, the Data Administrator/Custodian is to complete CIS Access Request Form indicating training has been completed. The records of training completion are housed in the College's employee learning management portal.

e. Within one business day of non-employment status of employee(s), ITS will be notified by the appropriate Data Owner/Administrator/Custodian of said status and complete the CIS User Action Form indicating the last date of employment. This will result in the immediate cancellation of access to administrative data, and ITS will ensure immediate termination of these services.

3. Revocation of Administrative Data Privileges

Administrative data access is a privilege that may be withdrawn by a Data Owner for violation of user responsibility. Suspected violations will be confidentially reported to the appropriate Data Owner. Confirmed violations of this procedure will be addressed under Procedure 12.19 – Personnel Actions for Violation of Employment Standards.

Original (signed) procedure is on file in the
Rowan-Cabarrus Community College President's Office
Dr. Carol S. Spalding, President

Originally:	Procedure No: 1.11
History Note:	Original Date: September 2003 Revisions: March 2004 Aug 2011 December 2012