


PROCEDURE

Subject:	Confidentiality	Number: 2.60.04
Source:	Vice President, Planning and Institutional Effectiveness	Reference (Rule #) 6HX14-2.60
President's Approval/Date:	 4/10/18	

PURPOSE: This procedure will help ensure compliance with applicable state and federal law, industry standards, and student, and public expectations.

SCOPE: This policy applies to:

- Users, systems, and locations;
- Employees, contractors, students, service providers; and
- Applies to all facilities.

POLICY STATEMENT: State College of Florida (SCF) sensitive information (e.g., confidential and Restricted information as defined in the SCF Data Classification Guidelines) in any format (i.e., verbal, written, or machine readable) that is accessible to SCF resources must be adequately protected. Confidential information (as defined in the SCF Data Classification Guidelines) should be maintained in a manner that ensures its privacy and security. Information must be consistently protected in a manner commensurate with its sensitivity, value, and criticality, including the following:

- a) At no time are SCF resources to divulge sensitive information about SCF systems.
- b) Non-staff system access must have permission from Information Technology management before system access is granted.
- c) Do not share your username and password!
- d) You are responsible for any activity conducted using your assigned user account.
- e) Anything saved or stored on company systems is considered SCF property.
- f) Do not remove any documents considered to be SCF confidential property from facilities without management permission.

NONCOMPLIANCE:

Any employee/contractor found to have violated this procedure may be subject to disciplinary action, up to and including termination of employment. Service providers found to have violated this procedure may be subject to financial penalties, legal action, and including termination of contract.