Data Security and Stewardship Policy

Rollins College takes seriously the proper use and protection of personal and institutional data. This policy pertains to all individuals who are involved in Rollins College business, whether they are paid or volunteers. Deans and Department heads are responsible for functioning as data stewards, ensuring that all individuals in the school/department are familiar with their responsibilities under this policy.

Information falls across a continuum of concern regarding its disclosure. While confidential information (e.g. social security number, bank accounts) must be given our closest attention, the College could also be harmed if other personal data are exposed (e.g. salaries, student grades). Therefore, protecting the College's data is everyone's responsibility.

Data Sources and Types

The majority of College data are maintained within our administrative system (i.e., Banner) and accessed either directly through the database interface or through a website (e.g., FoxLink, Blackboard). Often, data are transferred into a spreadsheet for further manipulation and sharing. Data may be collected on forms (electronic or paper) and stored within email accounts, in file cabinets, or on a workstation or server. Regardless of the way that the data are obtained and stored, all College data must be maintained in a secure manner.

College data fall into two main types: personal information and institutional information. Personal information includes, but is not limited to, social security and ID number, financial information, grades, and health records. Directory information (e.g., home address, telephone number, email address) is not confidential, unless an individual has asked that it be kept confidential. Institutional information includes, but is not limited to, College finances, personnel records and teaching evaluations.

Social Security Number

Federal and state law requires the collection of social security number (SSN) for certain purposes. However, widespread use of a person's SSN is a major privacy concern. With incidents of identity theft increasing, the protection of everyone's personal identity is important and steps are taken to protect everyone's information.

It is Rollins College policy that any report, web page or data extract will NOT contain SSNs unless required by law or by prior approval of senior management of Rollins College. This includes those specialized reports that contain parts of the SSN.

By law, Rollins College must collect and maintain SSNs for reporting and communicating to various legitimate agencies. It is therefore imperative that each person's SSN is recorded accurately within the database.

Permissions

Each College office and the personnel within that office have access to only those data they need to efficiently conduct College business. An individual may only access, manipulate or change data as required to fulfill their assigned duties. Level of data access is controlled through permissions assigned in the administrative system and to department folders on the server. Permissions are granted to individuals when a formal request is made (via a request for service) to Information Technology by the dean, department head or vice president.

Individuals are not allowed to circumvent the level of data access given to another individual by providing them access to data that they could not view themselves.

Securing Data: On-Campus

Individuals must be cognizant of maintaining the security of all College data, with special concern for confidential information. This includes both hard copies and digital copies of data, whether on a desktop/laptop computer or a personal digital assistant/ smartphone (PDA).

Hard copies

Hard copies must be properly stored within department offices, in locked file cabinets whenever possible, and these offices must be locked when they are not occupied. Any piece of paper that includes these data must be shredded prior to disposal.

Digital copies

Whenever possible, College data should be maintained on a College server. This would mean the data are kept within the administrative system or within a department network folder. Securing these data require that every individual completely logs off of the administrative system and the campus network before leaving their computer unattended.

At times, individuals may move data from the network and onto the hard drive of their workstation. These instances should be for very limited time frames and the data should be returned to the network and deleted from the hard drive before the computer is left unattended. Data left on the hard drive of the workstation is accessible to anyone who can gain access to the workstation, no permissions required.

Sharing data

Data files are often shared among individuals within the same office and across offices. Within an office, the department network folder is the most secure way in which to share files. A network folder is also the most secure way to share data across offices. A project-based network folder can be created and appropriate permissions assigned. A Blackboard course could also be created for a project.

Small amounts of confidential data may also be transferred between offices via email, on a CD or on a thumb drive. Non-password protected emails may contain Rollins College ID numbers, but must never

contain a social security number. At a minimum, emails that contain confidential information should be password-protected. The password should be sent in a separate email. Both parties should be sure to completely delete the message from their Inbox, Sent and Trash folders once they have transferred the data, including any copies on their PDA. Data files stored on CDs and thumb drives should be deleted after the transfer. CDs must be destroyed prior to disposal.

Securing Data: Off-Campus

Accessing data while off-campus requires even greater diligence than when on-campus. Department heads must ensure that any employee given the ability to do so must be aware of the vulnerability that the College may suffer if these data are lost while not on campus property.

If an employee does lose data while off-campus (laptop, PDA or file folder is stolen/missing) s/he must notify her/his supervisor immediately. The supervisor must then notify their Vice President and the Chief Information Officer (CIO). The CIO is responsible for responding to the security incident using established protocols.

Hard copies

There should be few instances when an individual leaves campus with a hard copy of College data. The individual who does so must maintain the absolute security of that copy and ensure that it is shredded upon disposal.

Digital copies

Remote access to the administrative server is available through Citrix. Individuals connecting to the administrative system while off-campus must exert the highest level of caution. Individuals who access their network folders from a College-owned laptop must be sure that they keep all of the data on the network and must not save any data onto the laptop hard drive.

Individuals should never connect using Citrix to the College network while using an unsecured wireless network.

3rd Party Contractors

Rollins College contracts with a variety of companies for services that require sharing confidential information. All such contracts must contain language that specifies that the contractor understands the confidentiality of the information that they are receiving, that they have the same responsibilities as Rollins College employees in maintaining the security of those data and that they understand the appropriate federal and state laws that govern the security of the specific data.

Policy Review

This policy is reviewed annually by the Enterprise Computing Group of Rollins College. After each review, the policy will be distributed to all faculty and staff at the College to alert them to any policy updates and to serve as a reminder of the importance of appropriate data stewardship.

Adopted April 20, 2010