

COLORADO COMMUNITY COLLEGE SYSTEM INFORMATION SECURITY PLAN

This Information Security Plan (“Plan”) describes Colorado Community College System’s safeguards to protect *covered data and information*.¹ These safeguards are provided to:

- Ensure the security and confidentiality of covered data and information;
- Protect against anticipated threats or hazards to the security or integrity of such information; and
- Protect against unauthorized access to or use of covered data and information that result in substantial harm or inconvenience to any customer.

This Information Security Plan also provides for mechanisms to:

- Identify and assess the risks that may threaten covered data and information maintained by the Colorado Community College System;
- Develop written policies and procedures to manage and control these risks;
- Implement and review the plan; and
- Adjust the plan to reflect changes in technology, the sensitivity of covered data and information and internal or external threats to information security.

Identification and Assessment of Risks to Customer Information

Colorado Community College System recognizes that it has both internal and external risks. These risks include, but are not limited to:

- Unauthorized access of covered data and information by someone other than the owner of the covered data and information
- Compromised system security as a result of system access by an unauthorized person

¹ *Covered data and information* for the purpose of this policy includes *student financial information* (defined below) required to be protected under the Gramm Leach Bliley Act (GLB). In addition to this coverage which is required under federal law, the Colorado Community College System chooses as a matter of policy to also include in this definition any credit card information received in the course of business by the System, whether or not such credit card information is covered by GLB. Covered data and information includes both paper and electronic records. *Student financial information* is that information that the Colorado Community College System has obtained from a customer in the process of offering a financial product or service, or such

information provided to the System by another financial institution. Offering a financial product or service includes offering student loans to students, receiving income tax information from a student's parent when offering a financial aid package, and other miscellaneous financial services. Examples of student financial information include addresses, phone numbers, bank and credit card account numbers, income and credit histories and Social Security numbers, in both paper and electronic format.

- Interception of data during transmission
- Loss of data integrity
- Physical loss of data in a disaster
- Errors introduced into the system
- Corruption of data or systems
- Unauthorized access of covered data and information by employees
- Unauthorized requests for covered data and information
- Unauthorized access through hardcopy files or reports
- Unauthorized transfer of covered data and information through third parties

Colorado Community College System recognizes that this may not be a complete list of the risks associated with the protection of covered data and information. Since technology growth is not static, new risks are created regularly. Accordingly, the CCCS-IT department will actively participate and monitor advisory groups such as the Educause Security Institute, the Internet2 Security Working Group and SANS for identification of new risks.

The Colorado Community College System believes the CCCS-IT current safeguards are reasonable and, in light of CCCS-IT current risk assessments are sufficient to provide security and confidentiality to covered data and information maintained by the System. Additionally, these safeguards protect against currently anticipated threats or hazards to the integrity of such information.

Information Security Plan Coordinators

The Vice President of Information Technologies and Director of Network Services have been appointed as the coordinators of this Plan. They are responsible for assessing the risks associated with unauthorized transfers of covered data and information and implementing procedures to minimize those risks to the Colorado Community College System.

Design and Implementation of Safeguards Program ***Employee Management and Training***

References of new employees working in areas that regularly work with covered data and information (Cashier's Office, Registrar, Development and Financial Aid) are checked by the hiring campus. During employee orientation, each new employee in these departments will receive proper training on the importance of confidentiality of student records, student financial information, and other types of covered data and information. Each new employee is also trained in the proper use of computer information and passwords. Training also includes controls and procedures to prevent employees from providing confidential information to an unauthorized individual, including "pretext calling"² and how to properly dispose of documents

that contain covered data and information. Each department responsible for maintaining covered data and information is instructed to take steps to protect the information from destruction, loss or damage due to environmental hazards, such as fire and water damage or technical failures. Further, each department responsible for maintaining covered data and information should coordinate with the Office of Legal Services on an annual basis for the coordination and review of additional privacy training appropriate to the department. These training efforts should help minimize risk and safeguard covered data and information security.

Physical Security

Colorado Community College System has addressed the physical security of CCCS-IT covered data and information by limiting access to only those employees who have a business reason to know such information. For example, personal customer information, accounts, balances and transactional information are available only to Colorado Community College System employees with an appropriate business need for such information. Loan files, account information and other paper documents are kept in file cabinets, rooms or vaults that are locked each night. Only authorized employees know combinations and the location of keys. Paper documents that contain covered data and information are shredded at time of disposal.

Information Systems

Access to covered data and information via Colorado Community College System's computer information system is limited to those employees who have a business reason to know such information. Each employee is assigned a user name and password. Databases containing personal covered data and information, including, but not limited to, accounts, balances, and transactional information, are available only to Colorado Community College System employees in appropriate departments and positions. Account and password information is only provided after receipt of documentation from the appropriate college/supervisor. Colorado Community College System will take reasonable and appropriate steps consistent with current technological developments to make sure that all covered data and information is secure and to safeguard the integrity of records in storage and transmission. CCCS-IT requires that all servers must be registered before being allowed through Colorado Community College System's firewall, thereby allowing CCCS-IT to verify that the system meets necessary security requirements as defined by CCCS-IT policies. These requirements include maintaining the operating system and applications, including application of appropriate patches and updates in a timely fashion. User and

² "Pretext calling" occurs when an individual improperly obtains personal information of CCCS customers so as to be able to commit identity theft. It is accomplished by contacting CCCS, posing as a customer or someone authorized to have the customer's information, and through the use of trickery and deceit, convincing an employee of the System to release customer-identifying information. System passwords are also required to comply with the Colorado Community College System Password Policy. In addition, an intrusion detection system has been implemented to detect and stop certain external threats, along with an Incident Response Policy for occasions where intrusions do occur. When commercially reasonable, encryption technology will be utilized for both storage and transmission. All covered data and information will be maintained on servers that are behind

the Colorado Community College System's firewall. All firewall software and hardware maintained by CCCS-IT will be kept current.

Management of System Failures

CCCS-IT has developed written plans and procedures to detect any actual or attempted attacks on Colorado Community College System systems and has an Incident Response Policy that outlines procedures for responding to an actual or attempted unauthorized access to covered data and information. This policy is available upon request from Dan Tacker_____, Director of Network Services.

Selection of Appropriate Service Providers

Due to the specialized expertise needed to design, implement, and service new technologies, vendors may be needed to provide resources that the Colorado Community College System determines not to provide on its own. In the process of choosing a service provider that will maintain or regularly access covered data and information, the evaluation process shall include the ability of the service provider to safeguard confidential financial information. Contracts with service providers may include the following provisions:

- An explicit acknowledgement that the contract allows the contract partner access to confidential information;
- A specific definition or description of the confidential information being provided;
- A stipulation that the confidential information will be held in strict confidence and accessed only for the explicit business purpose of the contract;
- An assurance from the contract partner that the partner will protect the confidential information it receives according to commercially acceptable standards and no less rigorously than it protects CCCS's own confidential information;
- A provision providing for the return or destruction of all confidential information received by the contract provider upon completion or termination of the contract;
- An agreement that any violation of the contract's confidentiality conditions may
- constitute a material breach of the contract and entitles Colorado Community College System to terminate the contract without penalty; and
- A provision ensuring that the contract's confidentiality requirements shall survive any termination agreement.

Continuing Evaluation and Adjustment

This Information Security Plan will be subject to periodic review and adjustment. The most frequent of these reviews will occur within CCCS-IT, where constantly changing technology and evolving risks mandate increased vigilance. Continued administration of the

development, implementation and maintenance of the program will be the responsibility of the designated Information Security Plan Coordinators who will assign specific responsibility for CCCS information technologies implementation and administration as appropriate. The Coordinators, in consultation with the Office of Legal Services, will review the standards set forth in this policy and recommend updates and revisions as necessary. It may be necessary to adjust the plan to reflect changes in technology, the sensitivity of student/customer data and internal or external threats to information security.