AURARIA HIGHER EDUCATION CENTER™

Policy Number 5.3.2

Chapter: Finance

Title: Information Technology Security

Division/Department: Finance/Information Technology

Policy Administrator: Director of IT

Adoption Date: February 26, 2025

Revision Dates:

1. PURPOSE

The information systems of Auraria Higher Education Center (AHEC) contain information from students, employees, business partners, government, and other sources, and serve to enable AHEC to accomplish its mission. The loss or misuse of information, and damage to information systems and databases, can cause substantial injury to AHEC and others in terms of financial loss, reputational damage, operational capability, and invasion of personal privacy. In addition, various laws and regulations require that AHEC observe certain policies and practices to safeguard its Data. This policy codifies the practices of AHEC in securing and protecting its Data to avoid loss or breach and associated risks.

2. DEFINITIONS

2.1. Constituent Institution: As defined in Colorado Revised Statutes (C.R.S.) § 23-70-101(b), an institution of higher education that is located on the AHEC campus, including Community College of Denver, Metropolitan State University of Denver, and University of Colorado Denver.

2.2. Data: All digital information that resides, even temporarily, in an AHEC Information Technology (IT) System or digital resource. Data is classified as follows:

2.2.1. Private Data – The most sensitive Data at AHEC, subject to the greatest protections. Because of legal, ethical, or other constraints, Private Data may not be accessed without specific authorization from the responsible Data Authority, and access may be granted only selectively as necessary to accomplish the legitimate business purposes of AHEC and its Constituent

Institutions. Private Data encompasses, without limitation, social security numbers, financial information including credit card information and bank account numbers, driver's license information, protected personnel information, proprietary research information, third-party proprietary information, personal health information, biometric data, and any other information that, through disclosure, would adversely affect an individual, AHEC or a Constituent Institution.

2.2.2. Restricted Data: Confidential or proprietary business or personal information requiring selective access under statutory, regulatory or contractual requirements. Restricted Data is intended for a specific use and should not be disclosed except to those who have explicit authorization to review such Data. Unauthorized disclosure of this information could have a serious adverse impact on AHEC, individuals or affiliates.

2.2.3. Public Data: Data explicitly made available to the public (e.g., available on open, public web pages, or in other publications sanctioned by AHEC).

2.2.4. Aggregated Data: Private Data that has been de-identified and compiled with other Data, such that the Data Subject can no longer be identified using any process, method, algorithm, or tool, or by reference to other published data.

2.3. Data Authority: A senior AHEC administrator (division chief, department head or equivalent) who is responsible for decisions related to Data access, use, storage, and protection of a particular type or collection of Data maintained in their area of responsibility. The AHEC IT Director is the overall Data Authority for the institution with authority to implement this policy and to prescribe procedures to assure the security of AHEC IT Systems.

2.4. Data Subject: An individual or entity whose Private or Restricted Data is present in an AHEC IT System or digital resource.

2.5. Information Technology (IT) System: IT Systems include AHEC-owned or controlled computing devices, networks, software, databases, services, and facilities. Examples include, but are not limited to, shared computer drives, network file shares, networkable copiers and scanners, programs and software.

2.6. Principle of Least Privilege: An accepted concept in IT that holds that data security architecture should be designed so that each individual or entity is granted the minimum system access, resources and authorizations that they need to perform their function.

3. POLICY

3.1. Information security at AHEC is managed by the Information Technology Department in the Division of Finance, but it is the responsibility of everyone having access to IT Systems and Data (users) to safeguard these digital resources and the information they contain. AHEC expects all members of the AHEC community (employees, contractors, and users) that have access to and responsibilities for Data to manage it as set forth in this policy with respect to collection, storage, disclosure, access, processing, destruction, and classification.

3.2. Data Hygiene: Users shall practice the following precautions to safeguard Private and Restricted Data:

3.2.1. Ensure that systems designed to host Public Data do not process, transmit, or store Private Data or Restricted Data unless all such protected Data is secured by passwords.

3.2.2. Remove Private Data and Restricted Data when no longer required for an AHEC business reason. See the AHEC Policy on Records Retention.

3.2.3. Follow the Principle of Least Privilege and do not access, transmit, share, or expose Private Data or Restricted Data when not necessary to conduct the business of the institution or required by law.

3.2.4. Mask or redact such Data on development or test systems.

3.3. General Prohibitions: Users shall observe the following prohibitions on actions involving Data:

3.3.1. Do not change Data about oneself or others for other than usual business purposes. Do not use information (even if authorized to access it) to support actions by which individuals might profit (e.g., use of AHEC Data for private business or financial purposes).

3.3.2. Do not disclose Data about individuals without prior supervisor authorization, unless it is Aggregated Data used for a business purpose.

3.3.3. Do not engage in “digital voyeurism” (e.g., tracking others’ activities, determining the source and/or destination of telephone calls or Internet protocol addresses, or exploring race and ethnicity indicators) unless authorized to conduct such analyses.

3.3.4. Do not circumvent the nature or level of data access given to others by providing access or data sets that are broader than those available to them via their own approved levels of access (e.g., providing a dataset of human resource information to a coworker who has a lesser level of access) unless authorized.

3.3.5. Do not facilitate another's unauthorized access to AHEC IT Systems or compromise the integrity of Data (for example, by sharing your password).

3.3.6. Do not violate AHEC policies or federal, state, or local laws in accessing, manipulating, or disclosing Data.

3.3.7. Server and Device Security: AHEC servers and devices shall be protected by the following security measures:

- Servers shall be housed in a physically secure facility where access is limited to only those individuals requiring access to perform routine or emergency maintenance on the IT System.
- Server-side computer virus protection shall be implemented and kept up to date.
- On servers and all devices, programs and applications installed/enabled shall be necessary to accomplish required AHEC business functions. Programs, services and applications, including social media platforms, used primarily for personal reasons are prohibited without express authorization from the IT Director.
- To the degree practicable, only operating systems and applications that provide high levels of security shall be used, system security features shall be enabled, and security updates (patches) shall be applied in a timely manner.
- To the degree practical, only secure connections and file transfers shall be allowed, for example by using secure web protocols (HTTPS), secure connections (e.g. SSL and SSH), and other secure mechanisms for connections (e.g. the AHEC VPN). This policy is particularly relevant when allowing access from external (non-AHEC) networks.
- Server files shall be backed up on a regular schedule, and off-site storage of back-ups in a secure location shall be maintained by AHEC IT. Backup systems shall be approved by the IT Director.
- Servers shall be scanned for operating system and application vulnerabilities on a regular schedule. Vulnerabilities detected shall be addressed in a timely manner.
- All storage media must be sanitized in accordance with the guidelines published by the National Institute of Standards and Technology (NIST) before release to outside agencies.

3.4. Passwords:

3.4.1. No user shall share a password or security token with any other user.

3.4.2. Unless different password requirements are built into an approved software or firmware program, the IT Director shall prescribe the minimum requirements for passwords to be used on IT Systems, and these are subject to change without notice.

3.4.3. Users shall be required to change their AHEC passwords at least annually, and whenever the IT Director determines there is a need to change a password.

3.5. Files and File Storage:

3.5.1. In general, users are responsible for their own files and ensuring that files containing critical Data are backed up in accordance with backup procedures established by the IT Director.

3.5.2. Files containing Private and Restricted Data shall be maintained on an AHEC server, not on a personal computer, external storage device (such as a memory stick or portable hard drive), or mobile device, except as authorized by the responsible Data Authority. Files containing Private or Restricted Data that are permitted to be kept on such devices shall be protected with strong encryption.

3.5.3. All types of physical media (disks, tapes, optical disks, memory sticks, memory cards, etc.) containing Private or Restricted data shall be disposed of properly, ensuring that the Data therein is not accessible after disposal and cannot be retrieved by any means. This may be accomplished either by degaussing or physically destroying the media (e.g., shredding), or both.

3.6. Data Authority Responsibilities: The Data Authority shall

3.6.1. Have access to and administrative responsibility for AHEC Data maintained in their area of responsibility, and broad-based knowledge of the purposes and means for collection, storage and use of such Data by AHEC employees and other users.

3.6.2. Classify the Data under their control and approve all uses of the Data.

3.6.3. Approve access to IT Systems by users that have a demonstrable business need.

3.6.4. Ensure that users are aware of this policy and any IT security procedures prescribed by the IT Director.

3.6.5. Immediately report any data security breach to the IT Director, as available, or another employee within the IT Department.

4. APPROVAL AND ADOPTION

This Policy has been reviewed and approved by the Board of Directors for the Auraria Higher Education Center.

Date: February 26, 2025

Approved by: /s/ Kate Barton
Chairperson of the Auraria Board