AURARIA CAMPUS POLICY

Policy Title:	Employee Computer Security		
Approval Authority:	IT Director		
Last Revised:	November 14, 2018	Category:	Internal Administrative Policy
Last Reviewed:	November 14, 2018	Effective:	March 2017

1. Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at the Auraria Higher Education Center (AHEC). These rules are in place to protect the employees and AHEC. Inappropriate use exposes AHEC to risks including virus attacks, compromise of network systems and services, and legal issues.

Security Policy Ownership and Responsibilities

The Information Technology Department is the assigned custodian of this security policy. It is the responsibility of the custodian to publish and disseminate this policy to all relevant AHEC system users (including vendors, contractors, and business partners). In addition, the custodian must see that the security policy addresses and complies with all standards AHEC is required to follow (e.g., Payment Card Industry Data Security Standard [PCI-DSS]). This policy will also be reviewed at least annually by the custodian (and any relevant data owners) and updated as needed to reflect changes to business objectives or the risk environment.

Questions or comments about this policy should be directed to the Information Technology Department Director.

2. Audience

This policy applies to employees, contractors, consultants, temporary staff, and other workers at AHEC, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by AHEC.

3. Policy

- **Employee Computer Usage**
  - Internet/intranet/extranet-related systems including, but not limited to, computer equipment, software, operating systems, storage media, network accounts providing electronic mail, www browsing, and FTP, are the property of AHEC. These systems are to be used for business purposes in serving the interests of the agency and of our clients and customers in the course of normal operations. Please review Human Resources policies for further details.
  - Effective security is a team effort involving the participation and support of every AHEC employee and affiliate who deals with information and/or information systems.

It is the responsibility of every computer user to know these guidelines and to conduct their activities accordingly.

- **General Use and Ownership**
  - All electronic correspondence by AHEC employees may be a public record under the Colorado Public Records Law, and may be subject to public inspection under CRS Section 24-72-203.
  - While AHEC's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the agency systems remains the property of AHEC. Because of the need to protect AHEC's network, management cannot guarantee the confidentiality of information stored on any network device belonging to AHEC.
  - Employees are responsible for exercising good judgment regarding personal use. Individual departments are responsible for creating guidelines concerning personal use of internet/intranet/extranet systems. In the absence of such guidelines, employees should consult their supervisor or manager.
  - For security and network maintenance purposes, authorized individuals within AHEC may monitor equipment, systems, and network traffic at any time.
  - AHEC reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.
- **Security and Proprietary Information**
  - If an employee has access to company sensitive or confidential information (e.g., financial data, payment data, credit card data, SSN, medical, etc.) from the workplace or via remote access technologies, the employee is prohibited from copying, moving, or storing this sensitive information on local hard drives or removable electronic media without explicit AHEC authorization.
  - Where possible, use strong encryption for passwords (a minimum of eight characters, with at least one upper case, lower case, numeric, and special character) to protect sensitive information stored on electronic media. Where credit card account data is involved, all handling of this data must comply with the PCI-DSS.
  - Do not reuse previously used passwords.
  - Change your password if there is any suspicion the password could be compromised.
  - Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System-level passwords should be changed according to accepted AHEC policy to meet PCI-DSS requirements where necessary.
  - All PCs, laptops, and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 30 minutes or less, or by logging-off when the host will be unattended.
  - Postings by employees from an AHEC email address to news groups should contain a disclaimer that the opinions expressed are strictly their own and not necessarily those of AHEC, unless posting is in the course of business duties.

- All hosts used by the employee that are connected to the AHEC internet/intranet/extranet, whether owned by the employee or AHEC, shall be continually executing approved virus-scanning software with a current virus database unless overridden by departmental or group policy.
- Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code. Contact the IT Support desk if you are unsure of the authenticity of email attachments.

- **Unacceptable Use**

  The following activities are prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may need to disable the network access of a host if that host is disrupting production services).

  Under no circumstances is an employee of AHEC authorized to engage in any activity that is illegal under local, state, federal, or international law while utilizing AHEC-owned resources.

  The following lists are not exhaustive, but attempt to provide a framework for activities that fall into the category of unacceptable use.

  System and Network Activities

  The following activities are strictly prohibited, with no exceptions:

  - Violations of the rights of any person or company protected by copyright, trade secret, patent, or other intellectual property, or similar laws or regulations including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by AHEC.
  - Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books, or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which AHEC or the end user does not have an active license is strictly prohibited.
  - Exporting software, technical information, encryption software, or technology in violation of international or regional export control laws is illegal. Appropriate management should be consulted prior to export of any material that is in question.
  - Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, malware, etc.).
  - Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
  - Using an AHEC computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
  - Making fraudulent offers of products, items, or services originating from any AHEC account.
  - Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

- Affecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
- Port scanning or security scanning is expressly prohibited unless prior notification to AHEC is made.
- Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
- Circumventing user authentication or security of any host network or account.
- Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with or disable a user's terminal session via any means, locally or via the internet/intranet/extranet.
- Providing information about or lists of AHEC employees to parties outside AHEC.

Email and Communications Activities

- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
- Any form of harassment via email, telephone, or texting, whether through language, frequency, or size of messages.
- Unauthorized use or forging of email header information.
- Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
- Creating or forwarding "chain letters," "Ponzi," or other "pyramid" schemes of any type.
- Use of unsolicited email originating from within AHEC's networks of other internet/intranet/extranet service providers on behalf of or to advertise any service hosted by AHEC or connected via AHEC's network.
- Posting the same or similar non-business-related messages to large numbers of usenet news groups (news group spam).

Social Media / Blogging

- Blogging by employees, whether using AHEC's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this policy. Limited and occasional use of AHEC's systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate AHEC's policy, is not detrimental to AHEC's best interests, and does not interfere with an employee's regular work duties.

- Blogging from AHEC's systems is also subject to monitoring.
- Employees shall not engage in any blogging that may harm or tarnish the image, reputation, and/or goodwill of AHEC, and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory, or harassing comments when blogging or otherwise engaging in any conduct prohibited by AHEC's Non-Discrimination and Anti-Harassment policy.
- Employees may also not attribute personal statements, opinions, or beliefs to AHEC when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent himself or herself as an employee or representative of AHEC. Employees assume any and all risk associated with blogging.
- Apart from following all laws pertaining to the handling and disclosure of copyrighted or export-controlled materials, AHEC's trademarks, logos, and any other AHEC intellectual property may also not be used in connection with any blogging activity.

Enforcement

Any employee found to have violated this policy might be subject to disciplinary action, up to and including termination of employment.

4. History and Updates

- November 14, 2018
  - Updated policy by placing in new format
  - Edited for basic language and updates to titles, departments, etc.