Black Hawk College
Administrative Guidelines

4-2 Computer Security and Appropriate Use

Approved by:

Insertion Date: 10/2002

Revision Date: 12/2005, 11/2007, 1/2016, 9/2016

Removal Date:

Board Policy: 8.90 & 9.60

Black Hawk College is committed to taking all reasonable measures to protect its information resources and to ensure these resources are used for their intended purpose. The following procedures and guidelines are designed to ensure responsible use of College information technology resources and to protect automated information and information resources against accidental or unauthorized disclosure, modification or destruction, as well as to assure the security, reliability, integrity, and availability of information at the College.

Black Hawk College reserves the right to extend, limit, restrict, or deny computing privileges and access to its information resources as well as to monitor the utilization of information resources.

Compliance with Administrative Guideline 4.2 is critical to protecting the College's information resources. Training is required annually for all employees, student employees, emeriti, and Board of Trustees members. Training is required within the first 30 days for new employees and student employees, and newly seated Board of Trustee members. Training will be conducted online and will consist of access to a copy of the Guideline, a quiz, and a certification. Certification is accessible once a passing score of 80% or above is attained, which is to be printed, signed to signify acceptance of the terms of the Guideline, and forwarded to the Information Technology Services (ITS) Department. The ITS Department is responsible for oversight and compliance. If certification is not received within 30 days, passwords and/or access and/or physical devices will be locked until the signed certification is received.

Definitions:

- Confidential Information is exempt from disclosure under provisions of the Freedom of Information Act, FERPA, HIPAA, PCI/DSS, or other applicable state or federal laws. Programs and files are confidential unless they have been explicitly made available to other authorized individuals. Examples include, but are not limited to, Passwords, Social Security Numbers, Personally Identifiable Information, Financial accounts, and/or Records or files denoted as "Confidential" (Financial Aid data, Payroll Direct Deposit, student refund accounts, etc.).
- Sensitive Information may be either public or confidential and requires a higher than normal assurance of accuracy and completeness. Sensitive information requires special precautions to ensure integrity and to protect it from unauthorized access, modification or deletion. Examples include, but are not limited to, Student Academic Records, Coursework.
- Information Resources include, but are not limited to, all College owned or managed:
    - Information that is transmitted, stored, printed, and/or processed by a computer system,
    - Security access codes including passwords,

- Information processing and telecommunications hardware, software, and computer media.

College information resources are not to be used for any activities that violate State or Federal law, College Policy, Administrative Guidelines, or to solicit non-College business for personal gain or profit. The College reserves the right to audit individual usage and practices concerning computer security and responsible use outlined herein for any reason at any time. Persons who become aware of any misuse are obligated to report it immediately as outlined in Appendix A: Incident Response.

Users of College information resources are subject to disciplinary action for all known violations. Violations of an illegal or criminal nature will be reported to the appropriate authorities.

- All College employees who violate any of the provisions of this Guideline are subject to disciplinary action up to and including termination of employment, in accordance with College Policy, Guidelines, and Union agreements.
- All students who violate any of the provisions of this Guideline are subject to disciplinary action consistent with the Student Handbook.
- All others who violate any of the provisions of this Guideline are subject to disciplinary actions up to and including removal from the premises and may be barred from access to some or all College information resources.

The College owns the email system provided for employees and the information transmitted and stored within it. Employees should have no expectation of privacy or confidentiality in any of their emails. Employee email may be monitored for policy, security, and/or network management reasons.

The remainder of this document further defines procedures and guidelines and is arranged as follows:

- The General section contains elements considered to be universal in nature.
- The remaining sections are in addition to the General section and are specific to types or groupings of Information Resources.

General (applies to all subsequent sections)

1. Security
    a. Employee access to College systems, applications, and secure network drives
        i. Minimum access to perform job duties.
        ii. Requested by employee's direct supervisor using the ITS Request Form or ITS Request Form for Adjunct (PT) Faculty Only. Forms are under the ITS Dept. section of Publications, Forms, and Manuals on myBlackHawk.
        iii. Vetted by system and/or application administrators responsible for the security of the system and/or application. Includes separation of duties where necessary to insure data integrity.
            1. If accepted, the administrator(s) will apply security and inform supervisor. Password is ready for employee pick up.
            2. If rejected, the administrator will confer with the supervisor, Co-CIO, and others deemed necessary to come to agreement on access level, note the outcome, and complete any security. The supervisor informs the employee, as necessary.
    b. Non-employee access to College systems and applications (e.g. auditors, consultants, vendor support, etc.).

i. Minimum access to perform non-employee responsibilities, such as auditing, consulting, etc.
ii. Requested by the department supervisor using the ITS Request Form. Forms are under the ITS Dept. section of Publications, Forms, and Manuals on myBlackHawk.
iii. Vetted by system and/or application administrators responsible for the security of the system and/or application. Includes separation of duties where necessary to insure data integrity.
    1. If accepted, the administrator(s) will apply security and inform supervisor. Password is ready for non-employee pick up.
    2. If rejected, the administrator will confer with the supervisor, Co-CIO, and others deemed necessary to come to agreement on access level, note the outcome, and complete any security. The supervisor informs the non-employee, as necessary.

c. Passwords
    i. When choosing a password, you are highly encouraged to follow these best practices:
        1. Use a combination of upper- and lower-case letters, numbers, and special characters as allowed by the application or system.
        2. Make it hard to guess – refrain from words found in a dictionary; family, friends, or pets names; favorite sports teams or other well-known personal favorite things or activities.
        3. Select a unique password for each application or system.
        4. Change all your passwords at least twice a year.
        5. Do not store passwords where visible or unsecured.
    ii. Your password is for your exclusive use. Do not share it with anyone.
    iii. If any BHC employee asks for your password, report it immediately to the Co-CIO.
    iv. When typing your password, ask people to look away from the keyboard.
    v. Do not attempt to learn another's password. Look away from the keyboard when others are typing their passwords.
    vi. If you believe your password (or passwords) has been learned or otherwise compromised, change it (or them) immediately and follow Appendix A: Incident Response.
    vii. If you witness or suspect someone is/was using another person's credentials, immediately follow Appendix A: Incident Response.
    viii. If you forget your password, contact the ITS Help Desk, x5555 or email 5555@bhc.edu, for assistance.
d. Virus/Malware
    i. Think before you click. Be wary, alert, and skeptical when using the Internet and email. If it looks too good to be true, or looks odd, it probably is. Unsolicited items are questionable.
    ii. If you suspect a College system has been infected, and/or it's acting abnormally, contact the ITS Help Desk or your instructor for assistance.
    iii. ITS will investigate in accordance with Appendix A: Incident Response.
    iv. If ITS informs you your account has been compromised, a technician will work with you to change your password(s) and any other remedial steps.
e. Transmission of Confidential or Sensitive information (e.g. email, website, other)

i. Information is to be transmitted only when absolutely essential.
ii. Data encryption of a minimum of 128 or 256+ bit strength must be used. For assistance, contact the ITS Help Desk.
iii. Target, or receiving system must be at least as secure as the sending system.
iv. Recipient must be authorized to view the data.
v. Transmission to external systems or help desks is prohibited.
vi. If you receive Confidential or Sensitive information that does not follow these protocols, immediately follow Appendix A: Incident Response.

f. Credit Card and PCI/DSS Information – refer to Credit Card Handling PCI/DSS Information Security Procedure in myBlackHawk, Employees tab, in the Publications, Forms, and Manuals section under Institutional Documents.

2. Loss/theft
   a. Report any lost or stolen technology-related equipment, devices, or storage containing College information resources to the BHC Police immediately.
      i. Include type of device(s), types of data stored, and device connectivity to College information resources.
      ii. Change password(s) immediately.
      iii. BHC Police alert the Co-CIO for execution of Appendix A: Incident Response.
3. Retirement/NLE/Job Change (employee and supervisor responsibilities)
   a. Supervisor to follow HR process for equipment turn-in.
   b. Supervisor to submit removal paperwork for all systems and/or applications to which the exiting employee has access as soon as the last date of employment is known. Failure to do so may result in disciplinary action. Fill out the Removal section of the ITS Request Form or ITS Request Form for Adjunct (PT) Faculty Only, noting email and/or electronic file retention/access requests. Forms are under the ITS Department section of Publications, Forms, and Manuals on myBlackHawk.
   c. Administrators responsible for the security of the system(s) and/or application(s) are to disable access on the last date of employment at the College, or the last day in the previous position at the College, or as noted on the removal form, or as soon after as is possible.

Mobile Communication (examples include, but are not limited to, cell phones, pagers)

1. College owned
   a. Subject to inspection by College-designated authority at any time. Includes but not limited to the employee's supervisor, BHC Police, ITS, etc.
   b. Required to password-protect.
   c. Required to have an active wipe service.
   d. No Confidential or Sensitive data storage on device/in the cloud.
   e. Follow the Loss/Theft section of this document immediately if lost or stolen.
2. Personally owned (stipend)
   a. Highly encouraged to password-protect.
   b. Highly encouraged to have an active wipe service.
   c. No Confidential or Sensitive data storage on device/in the cloud.
   d. Follow the Loss/Theft section of this document immediately if lost or stolen.
3. Personal
   a. Highly encouraged to password-protect.
   b. Highly encouraged to have an active wipe service.
   c. No Confidential or Sensitive data storage on device/in the cloud.

Workstations (PCs, Apple computers, etc.)

1. College owned
    a. Subject to inspection by College-designated authority at any time. Includes but not limited to the employee's supervisor, BHC Police, ITS, etc.
    b. Password-protected.
    c. Storage of authorized Confidential or Sensitive info is ok.
    d. Data should be stored on the network drives (example: users H: drive and/or the departmental drive) for automated backup.
    e. Follow the Loss/Theft section of this document immediately if lost or stolen.
    f. Do not leave unattended when logged in – lock your screen. Any mischief done under your credentials is your responsibility.
    g. Administrator rights can be requested from ITS using the ITS Account Request Form. These rights are granted as deemed necessary. All software should be approved by ITS before installation.
    h. It is expected that this device is used for College business only.
2. Labs
    a. Subject to inspection by College-designated authority at any time. Includes but not limited to the lab supervisor, Faculty, BHC Police, ITS, etc.
    b. Password-protected.
    c. Storage of authorized Confidential or Sensitive info is prohibited.
    d. Data should be stored on the network drives (example: users H: drive) or removable storage (see Removable Storage section).
    e. Follow the Loss/Theft section of this document immediately if lost or stolen.
    f. Do not leave unattended when logged in – lock your screen. Any mischief done under your credentials is your responsibility.

Mobile Equipment – laptop

1. College owned
    a. Subject to inspection by College-designated authority at any time. Includes but not limited to the employee's supervisor, BHC Police, ITS, etc.
    b. Encrypted, password-protected is ITS standard configuration. Any modification by other than authorized ITS staff is prohibited.
    c. Storage of authorized Confidential or Sensitive info is ok.
    d. Data should be stored on the network drives (example: users H: drive and/or the departmental drive) for automated backup.
    e. Employee is required to attach to College network at least monthly to receive security and other software updates. ITS will audit monthly and report non-compliance to the employee and his/her supervisor. Repeating non-compliance will be escalated to the next supervisor and HR.
    f. Follow the Loss/Theft section of this document immediately if lost or stolen.
    g. Remote connection (VPN) to the College's private network can be requested. Refer to the Security, Employee Access to College systems section.
    h. Do not leave unattended when logged in – lock your screen. Any mischief done under your credentials is your responsibility.
    i. Administrator rights can be requested from ITS using the ITS Account Request Form. These rights are granted as deemed necessary. All software should be approved by ITS before installation.

    j. It is expected that this device is used for College business only.
2. Personal
    a. Encryption/password protection is highly encouraged.
    b. Storage of Confidential or Sensitive information is prohibited.
    c. Storage of other College information resources is discouraged.
    d. Remote connection (VPN) to the College's private network is prohibited.

Mobile Equipment - tablet

1. College-owned
    a. Subject to inspection by College-designated authority at any time. Includes but not limited to the employee's supervisor, BHC Police, ITS, etc.
    b. Encrypted, password-protected is ITS standard configuration. Any modification by other than authorized ITS staff is prohibited.
    c. Storage of authorized Confidential or Sensitive info is ok.
    d. Data should be stored on the network drives (example: users H: drive and/or the departmental drive) for automated backup.
    e. Employee is required to attach to College network at least monthly to receive security and other software updates. ITS will audit monthly and report non-compliance to the employee and his/her supervisor. Repeating non-compliance will be escalated to the next supervisor and HR.
    f. Follow the Loss/Theft section of this document immediately if lost or stolen.
    g. Remote connection (VPN) to the College's private network can be requested. Refer to the Security, Employee Access to College systems section.
    h. Do not leave unattended when logged in – lock your screen. Any mischief done under your credentials is your responsibility.
    i. Administrator rights can be requested from ITS using the ITS Account Request Form. These rights are granted as deemed necessary. All software should be approved by ITS before installation.
    j. It is expected that this device is used for College business only.
2. Personal
    a. Encryption/password protection is highly encouraged.
    b. Storage of Confidential or Sensitive info is prohibited.
    c. Storage of any College information resources is discouraged.
    d. Remote connection (VPN) to the College's private network is prohibited.

External Systems (systems, software, or services not College-owned, managed, or sanctioned)

1. The Learning Management System used by BHC is Canvas or myCourses in myBlackHawk.
2. Any connection to College-owned information resources is prohibited unless prior approval is obtained. Process: complete a form, ITS reviews and responds to requestor and their supervisor/dean.
3. Storage of Confidential or Sensitive information is prohibited.
4. Storage of information resources that are not Confidential and not Sensitive is prohibited unless prior approval is obtained. Process: complete a form, ITS reviews and responds to requestor and their supervisor/dean.

Shared Network Storage

1. N: drive
    a. Accessible by all employees.

    b. Storage of Confidential or Sensitive information is prohibited.
2. Departmental or Work Team drives
    a. Access is limited to requested employees.
    b. To request a drive, use the ITS Request Form. Forms are under the ITS Dept. section of Publications, Forms, and Manuals on myBlackHawk.
    c. Access to the drive is requested by the drive owner and the employee's direct supervisor using the ITS Request Form or ITS Request Form for Adjunct (PT) Faculty Only. Forms are under the ITS Dept. section of Publications, Forms, and Manuals on myBlackHawk.

Removable Storage (USB, thumb drive, external hard drive, CDs, DVDs, etc.)

1. Encryption is highly recommended. Contact the ITS Help Desk for assistance.
2. Password-protection is highly recommended. Contact the ITS Help Desk for assistance.
3. Storage of Confidential or Sensitive data is strongly discouraged.
4. Follow the Loss/Theft section of this document immediately if lost or stolen.

Appendix A: Incident Response

1. In the event of a suspected security violation, students are to alert the Dean of Students and employees are to alert the Co-Chief Information Officer (Co-CIO) or direct supervisor immediately. All incidents are to be reported.
2. The Dean of Students or the supervisor is to alert the Co-CIO and aid the investigation as required by the Co-CIO or designee.
3. The Co-CIO or designee will carry out an initial investigation of the suspected security violation.
4. The Co-CIO or designee will invoke the Red Flags procedure if it appears to be Red Flags related.
5. The Co-CIO or designee will inform BHC Police if it appears to be illegal.
6. Upon confirmation that a security violation has occurred, the Co-CIO will alert the college administration and begin informing all relevant parties that may be affected. Mitigation will also begin if it is not already in progress.