

Computer Security and Responsible Use

1. General Statement. Automated information and information resources owned or managed by Black Hawk College provide access to information technology and resources for students, faculty members, staff members, and other authorized users within institutional priorities and financial capabilities. Although Black Hawk College takes measures to safeguard integrity and confidentiality, it in no way guarantees the safety or security of information resources. Black Hawk College disclaims liability for the unauthorized interception, use, misuse, damage or destruction of information resources. No student, faculty member, staff member, or authorized user shall seek to hold Black Hawk College liable for damage resulting from unauthorized interception, use, misuse, damage or destruction of information resources. Each authorized user shall hold Black Hawk College harmless and indemnify it for any expense or loss caused by his/her own unauthorized interception, use, misuse, damage, or destruction of information resources, or by his/her violation of this Policy.

It is the policy of Black Hawk College to take all reasonable measures to protect its information resources and to ensure these resources are used for their intended purposes. The administration of the College will develop and implement guidelines and procedures to ensure responsible use of its 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. Such guidelines and procedures shall not infringe upon the academic freedom rights and responsibilities of faculty members as stated in Board policy.

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 by authorized users.

2. Definitions. The following definitions apply to this policy:
 - (a) “Information Resources” include, but are not limited to, all College owned or managed:
 - information processing and telecommunications hardware, software, and computer media;
 - security access codes including passwords and;
 - information that is transmitted, stored, printed, and/or processed by a computer system.
 - (b) An “Authenticated User Account” is an account established on an information resource which includes a user name and password and is

designed to uniquely identify a specific individual to the information system for the purpose of providing resources to that user.

- (c) “Confidential Information” maintained by the College is exempt from disclosure under provisions of the Freedom of Information Act or other applicable state or federal laws. Programs and files are confidential unless they have been explicitly made available to other authorized individuals.
 - (d) “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.
3. Responsible Use. As a learning organization, it is within the scope of responsible use to utilize College information resources, including e-mail, for personal and professional development activities, subject to the provisions that these activities: 1) do not interfere with college operations, 2) do not interfere with the ability of an employee to meet all job expectations, 3) do not unduly interfere with ability of other students to accomplish coursework, 4) do not impose a burden on College resources, and 5) are not among the prohibitions listed in Section 4 below.
4. Prohibitions. The following activities are specifically prohibited by this policy:
- (a) Use of College information resources to originate, view, disseminate, or store material that: is libelous; violates copyright or other intellectual property law; intimidates, threatens, or harasses individuals or groups in violation of law or College Policy; endangers the security of information resources; or violates other state or federal law or College Policy.
 - (b) Use of College information resources in the operation of a commercial business or service. Exempted from this prohibition are scholarly and academic endeavors which are allowed subject to provisions of bargaining unit agreements and/or handbooks. Also exempted is the occasional posting of articles for sale on electronic “bulletin boards.”
 - (c) Use of College information resources to gain access to sensitive or confidential information which is not required to perform job duties.
 - (d) Attempting to circumvent system guidelines or security or invade the privacy of individuals.
 - (e) Deliberately attempting to degrade the performances of a computer system or information resource; damage hardware, software or data; or to deprive

authorized personnel of resources or access to any College computer system.

- (f) Allowing another to use an assigned authenticated user account or using the authenticated user account of another individual without appropriate prior supervisory approval. Specifically prohibited are:

- revealing passwords either verbally or in writing;
- negligent disclosure of passwords such as posting passwords on or about workstations; and
- attempting to learn the password of another user.

5. Violations and Discipline. All College employees who violate Section 4 of this policy are subject to disciplinary action up to and including termination of employment. An employee who is subject to disciplinary action based on an allegation of a violation of this policy shall be entitled to full due process rights provided under the appropriate grievance process for his/her classification.

All students who violate Section 4 of this policy are subject to disciplinary action consistent with the student handbook.

6. Certification. All users, by accessing any College information resources are certifying that they understand and accept the provisions of this Policy and may be subject to disciplinary action for infringements of this policy. "Users" may be defined as students, employees or community members.

ADOPTED 4/17/97, B.R. #5788
AMENDED 4/28/05, B.R. #7064