Acceptable Use of Information Systems

Information Technology Division | helpdesk@hcc.edu | 413.552.2075

PURPOSE

This policy delineates the permissible use of information resources at Holyoke Community College. It is applicable to all HCC account holders, employees, students (with specified exceptions), contractors, consultants, temporary workers, and other staff at Holyoke Community College, as well as all individuals affiliated through third-party contractors.

This policy applies to all data and equipment that is owned or leased by Holyoke Community College.

The purpose of this policy is to protect employees, partners and HCC against internal and/or external exposure of confidential information, malicious activity, including the compromise of systems and services, legal issues, financial loss, and damage to reputation by individuals, either knowingly or unknowingly.

SCOPE

Personnel using data and information resources (including but not limited to Internet/Intranet/Extranet-related and core systems, computer equipment, software, operating systems, storage media, and network accounts providing electronic messaging), must use them for business/academic purposes in accordance with their roles and responsibilities, serving the interests of HCC and the students in a legal, ethical, responsible, and secure manner, with respect for the rights of others.

POLICY

It is the responsibility of every user of information resources to know the Information Security Policies and the acceptable use of information resources, and to conduct their activities accordingly.

General Use

- Safeguard user accounts and passwords, and use them only as authorized
- Respect all pertinent licenses, copyrights, contracts, as well as other restricted and proprietary resources
- To accommodate employees, Holyoke Community College understands employees will access the Internet for personal needs periodically
- It is expected that employees will exercise good judgment regarding the reasonableness of personal use and any question regarding appropriate use will be decided by management
- Notify the appropriate system, network and/or security administrator(s) of any suspected or actual security violations/incidents
- Secure all unattended workstations from unauthorized viewing or use
- All workstations must be configured to automatically lock after 10 minutes of inactivity and users should log off or lock their machines during extended periods of inactivity

Unacceptable Use

The following unacceptable activities are by no means exhaustive, but attempt to provide a framework for activities that are strictly prohibited:

- Damaging computer systems
- Preventing another user from authorized resources
- Accessing unauthorized systems or data resources, or utilizing functions that are not necessary for the performance of the employee's duties
- Revealing account passwords to others. Employees who receive usernames and passwords must keep their usernames and passwords confidential and must not share that information with others.
- Using another person's computer account, with or without their permission
- Providing information about employees to parties outside HCC
- Providing protected student or vendor information to any unauthorized person
- Intentionally corrupting, misusing, or stealing software or any other computing resource
- Sending unsolicited (SPAM) electronic messaging (e.g. email) and chain letters
- Forging electronic messaging header information
- Using electronic messaging, telephone or other communication method, to actively engage in procuring, viewing, or transmitting material that is in violation of sexual harassment or hostile workplace laws
- Accessing, editing, deleting, copying, or forwarding files or communications of another user in any media (e.g., paper, electronic, video, etc.), unless assigned as a job requirement or with prior consent from the file owner
- Deleting, editing, or copying files in another person's computer or electronic messaging account
- Illegal use, including duplication or distribution of copyrighted or HCC proprietary material, including electronic, hardcopy, audio, and video in any medium
- Employees are forbidden to install software on their computers without the prior approval of their supervisor
- Procurement of or use of any Software as a Service (SaaS) providers without the approval of Information Technology
- Implementation of any information technology component, product or service without the approval of and involvement from IT
- Removing software from systems, unless assigned as a job requirement or prior consent from Information Technology is obtained
- Circumventing any of the information security measures of any host, network or account without officer approval for emergency business purposes
- Using resources for personal benefit
- Introducing malicious programs into the information systems
- Unauthorized modification of configuration files
- Knowingly executing a program that may hamper normal activities, without prior authorization
- Operating a wireless network or allowing other computers to connect to your computer wirelessly
- Employees must not reveal any information about HCC's students or employees which is not already publicly available without expressed permission from their manager
- Unauthorized disclosure of confidential information to individuals outside HCC and to individuals within HCC without a business need, legal or regulatory requirement

- Disclosure of Personally Identifiable Information (PII) such as social security numbers, bank/credit card numbers, driver's license/id numbers, etc. and any other information classified as confidential, personal or sensitive to any unauthorized individual within HCC without a business need
- Disclosure of PII to any individual outside of HCC unless there is a legal or regulatory requirement
- Unencrypted transmission of PII (and confidential, personal and sensitive information), trade secrets, proprietary financial information and financial account numbers such as in the body of or an attachment to an electronic message, via FTP, via instant messenger or via fax
- Storing confidential information including PII (and confidential, personal and sensitive information), trade secrets, proprietary financial information or financial account numbers on laptop computers and mobile computing devices unless no alternative exists and then it must be encrypted
- Unauthorized application downloads from the internet are strictly forbidden. If applications are required for business use, contact IT and arrangements may be made
- Under no circumstance is an employee authorized to engage in any activity deemed illegal by international, federal, state, or other local laws while utilizing HCC assets
- Under no circumstances may an employee disable anti-virus software or alter anti-virus software settings
- Under no circumstances may user of HCC equipment disable firewall software or alter firewall software settings
- HCC account holders should not open any electronic messaging attachments that are not expected, or are from unknown addresses, or appear in any way suspicious
- Employees can only use HCC accounts to post official / approved publicly accessible messages. Employees should never use a personal account to represent the college.
- HCC account holders may not perform vulnerability scans, monitor network traffic, attempt to elevate rights or privileges, or gain access to information not expressly intended for them, unless explicitly authorized to do so by the CIO or their designee.

To ensure compliance with this policy, Holyoke Community College may perform periodic monitoring of systems, networks, and associated equipment at any time. Personnel using any Holyoke Community College information resources consent to disclose the contents of any files or information stored or passed-through Holyoke Community College equipment. All data contained on or passing through HCC's assets is subject to monitoring and remains the property of HCC at all times.

Other provisions:

- Explicit management approval must be provided for use of IT resources by employees or third parties
- Explicit management approval is required in order to add a new device to the network
- Authentication is required in order to use any technology
- Accessing unauthorized systems, data resources, or utilizing functions that are not necessary for the performance of the employee's job functions shall be prohibited
- A list of all devices and personnel with access shall be maintained
- A list of acceptable uses of technology and acceptable network locations shall be maintained
- A list of HCC approved products shall be maintained

References

<table>
<tr><td>Frameworks</td><td>
<table>
<tr><th>Name</th><th>Reference</th></tr>
<tr><td>NIST</td><td>AC-8 System Use Notification
IR-6 Incident Reporting
PL-4 Rules of Behavior
PS-6 Access Agreements
PS-8 Personnel Sanctions</td></tr>
<tr><td>ISO 27001</td><td>A.8.1.3 Acceptable use of assets
A.16.1.2 Reporting information security events</td></tr>
</table>
</td></tr>
<tr><td>Regulations and Requirements</td><td></td></tr>
<tr><td>Supporting Standards and Procedures</td><td></td></tr>
</table>