ICCCSSO
Computer Hacking

Do any of you have a policy to address computer hacking by someone who is visiting your campus and is not a student? Just wondering if you have precautionary language in your Code of Conduct or elsewhere on your campuses to address this behavior.	
Chad Flannery Dean for Student Services and Enrollment Southeastern Illinois College	I don’t know how many responses that you’ve received, but here at Southeastern, we have an IT acceptable use policy. It can be found on page 41 of our catalog found here: http://www.sic.edu/files/uploads/global/Catalog/Catalog.pdf. We fold violations into our Standards of Conduct procedures.
Dick Vallandingham Black Hawk College	No just general computer usage rules applied to all users
Dr. Carol Cowles Dean of Student Services and Development Elgin Community College	Non-student behavior would not be covered by our code of conduct. Visitors/guests on our campus would be subject to criminal charges. CC
Randy Greenwell Spoon River College	**Prohibited Acts:** The use of Spoon River College technology and network services for illegal or unethical acts or in violation of Spoon River College policy is strictly prohibited and subject to the discipline up to and including termination of employment. The examples listed are not exhaustive and may change from time to time as technology and applications change. If you are unsure whether any use or action is permitted, please contact the Chief Information Officer for assistance. Examples of prohibited acts include: a. Seeking, accessing, viewing, submitting, transmitting, receiving, publishing, displaying, or posting any defamatory, inaccurate, abusive, obscene, profane, sexually oriented or explicit, threatening, racially offensive, harassing, or illegal material. b. Attempting to obtain unauthorized access or circumventing user authentication or security of any host, network or account ("cracking"). This includes accessing data not intended for the

	user, logging into a server or account the user is not expressly authorized to access, or probing the security of systems or networks. c. Excessive use of technology resources for "frivolous" purposes, such as playing online games or downloading files. This causes congestion of the network or may otherwise interfere with the work of others, especially those wanting to use public access PCs or network and Internet resources. d. Unauthorized communication of personal information, such as home addresses, telephone numbers, Social Security numbers, or information protected by federal or state law of employees or students including but not limited to accessing, transmitting, receiving, or seeking unauthorized, confidential information or information protected by federal or state law about students or colleagues. e. Sending messages or materials (pictures, internet links, etc.) that violate the Spoon River College anti-harassment policy. f. Engaging in illegal activities or encouraging others to do so. Downloading, transmitting, selling, or providing information determined to be confidential or proprietary to Spoon River College. h. Conducting unauthorized business including, but not limited to, conducting your own personal business (i.e. business for another institution or business). i. Unauthorized access of others' folders, files, work, or computers. Intercepting communications intended for others. j. Causing harm or damaging others' property such as: Downloading or transmitting copyrighted materials without permission; (Note: Even when materials on the network or the internet are not marked with the copyright symbol,ã users should assume all materials are protected under copyright laws—unless explicit permission to use the materials is granted.) · Using another employee's password; · Intentionally uploading and/or disseminating a computer virus, harmful component, or corrupting data; using software that is not licensed or approved by the Spoon River College IT Office. k. Jeopardizing the security of the network or by disclosing or sharing passwords. l. Accessing or attempting to access materials that contain illegal information or are in violation of Spoon River College anti-harassment policy. m. Engaging in non-Spoon River College work-related activity during working hours.

n. Technology and network services may not be used to solicit or lobby for commercial ventures; personal, religious or political causes; outside organizations; or other non-job-related solicitations.

o. Installation of software on any Spoon River College computer or network without prior approval from the Chief Information Officer or Director of Technology Services, who will perform or supervise all approved installations.

4. **Abuse of Privileges/Policy Violation/Discipline:** Abuse of privileges and any policy violation or violation of regulations affecting this policy may result in revocation system access and/or disciplinary action per the College’s discipline policy. Users may also be held personally liable for any violations of this policy.

5. **Personal Responsibility:** By accepting account passwords and using Spoon River College’s communication equipment, network, e-mail system or internet access, user agrees to adhere to this policy. Additionally, user agrees to report any observed or misuse of same to the Human Resources Office.

Privacy and College Rights: The College’s technology and network services are Spoon River College property. Additionally, all communications sent or received on these devices are and remain the property of Spoon River College. Network and e-mail services, along with college provided internet access are provided as tools to use in conducting the College’s business. **Spoon River College reserves the right to monitor, inspect, copy, review, and store, at any time and without prior notice, any and all usage of the network, e-mail and history of internet access**. This includes any and all materials, files, information, software, links, communications, and other content transmitted, received, or stored in connection with this usage. All such information, content, and files are the property of Spoon River College and users should have no expectation of privacy regarding them. The IT or Human Resources Offices may review files and intercept communications for any reason, including but not limited to, maintaining system integrity and ensuring employees are using the system in a manner consistent with this policy.

7. **Responsibility of Enforcement:** All supervisors are responsible to enforce this policy. Also, employees who discover a violation of this policy shall notify their supervisor, the Human Resources Office or the Chief Information Officer (CIO).

Lesley Frederick Vice President, Student Services Lincoln Land Community College Esteban Cruz, MBA Chief Information Officer Lincoln Land Community College	We don’t have a policy dealing directly with computer hacking by a third party. We do, however reference to computer hacking in Policy 10.4 – Employee’s Role in Security. We basically disable any user account believed to be compromise. Here is a link to our IT policies: http://www.llcc.edu/Portals/0/Board/Policy/Chapter%2010%20Information%20Technology.pdf Computer hacking is illegal, so if the perpetrator is clearly identified, the incident could be reported to the police.
Dr. Normah Salleh-Barone VP for Student Development Moraine Valley Comm. College Kent Marshall Assistant Dean Code of Conduct & Student Life Moraine Valley Comm. College	Our Code of Student Conduct is only applicable to those we define as students. The MVCC Police should be called if anyone else is caught hacking into a computer and they could proceed with criminal charges and trespass the individual from campus if necessary.

U:\Student Services\ListServe--Computer Hackers.docx