Policy Number	701.000

installation of any copyrighted software for which CIU 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. The 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, email bombs, 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 CIU computing resources to harass, defame, and/or threaten others via written, recorded, or electronically retrieved or transmitted communications (including on Web sites and social media). Actively engaging in procuring or transmitting material that is in violation of CIU's sexual harassment or hostile workplace policies is expressly prohibited as stated in the Employee Handbook in the "Standards of Conduct and Corrective Action," and "Harassment (Including Sexual Harassment)" policies.
- Making fraudulent offers of products, items, or services originating from any CIU account.
- Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
- Effecting 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 duties 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 CIU 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, CIU students, alumni, employees, and donors to parties outside CIU without permission.

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 paging, 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 CIU's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by CIU or connected via CIU's network.
- Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

Employee Social Media

- Social media can be a fun and rewarding way to share your life and opinions with family, friends and co-workers around the world. While CIU does not discourage online communication, this type of technological communication is personal and not corporate, and use of social media also presents certain risks and carries with it certain responsibilities. To assist you in making responsible decisions about your use of social media, we have established these guidelines for appropriate use of social media. Whenever necessary, CIU may take steps to protect its reputation and business information.