Policy Number	701.000
Policy Title	IT ACCEPTABLE USE POLICY
Responsible Officer	Vice President, Information Technology
Responsible Office	Information Technology Services
Summary	CIU's intentions for publishing an Acceptable Use Policy are not to impose unnecessary restrictions within CIU's established culture, but to protect the corporation. CIU is committed to protecting employees, partners and the corporation from illegal or damaging actions by individuals, either knowingly or unknowingly. The property of CIU includes but not limited to *Internet/Intranet/ Extranet*-related systems, databases, computer equipment, *software*, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP. These systems are to be used for business purposes in serving the interests of CIU, and of our clients and customers in the course of normal operations. This includes personally-owned *software* and hardware when conducting corporate business. Please review employee and student handbooks for further details. Effective security is a team effort involving the participation and support of every CIU employee and partner who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.
Definitions	*Blogging*-short for web log, *blogging* is the act of posting commentaries on a personal online journal. *Chain letter*-a letter that is sent successively to several people. *Email bombs*-a form of net abuse consisting of sending huge volumes of email to an address to overflow email accounts. *Internet/Intranet/Extranet*-worldwide and private/restricted networks. *Junk mail*-third class mail consisting of advertising. *Packet spoofing*-Creation of IP packets with a false or forged source IP address with the purpose of concealing the identity of the sender or impersonating another computing system. *Pinged flood*-When a hacker or other malicious agent sends countless or repeated ping requests to your computer or server to overwhelm your data traffic with packets. *Ponzi*-investment scheme email involving fraudulent payments. *Pyramid*-fraudulent scheme involving the recruitment of people to generate substantial revenue for top level investors. *Software*-The term *software* represents wide range of applications such as licenses, desktop *software* and server *software*. *Spam*-Unauthorized and/or unsolicited electronic mass mailings. *Trojan horse code*-an extremely harmful *virus* code. *Virus*-a *software* program capable of damaging files and other computer programs.
Approving Body	Corporate Technology Steering Committee, Human Resources Committee; Academic Council, Administrative Council
Approval Date	August 25, 2014 701.000 – July 10, 2017; May 8, 2017
Last Revision	September 1, 2016
Re-evaluation Date	Fall 2021
Departmental Impact	All CIU, Ben Lippen, and Pine View Employees

Failure to follow the following policy may result in disciplinary action, including termination of employment.

Policy
This policy applies to employees, students, contractors, consultants, temporaries, and other workers at CIU, including all personnel affiliated with third parties. This policy applies to all technology used for corporate business purposes.

- While CIU desires to provide a reasonable level of privacy, users should be aware that the data created for corporate business purposes remains the property of CIU. Because of the need to protect CIU's corporate business information, the personal privacy of data created by users cannot be assured.
- Employees are responsible for exercising good judgment regarding the reasonableness of personal use.
- For data or information considered sensitive or vulnerable, see CIU's "Confidentiality of Information" policy in the *Employee Handbook*.
- Authorized individuals within CIU may monitor equipment, systems and network integrity at any time.
- CIU reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

Security and Proprietary Information

- The user interface for information contained on *Internet/Intranet/Extranet*-related systems should be classified as either confidential or not confidential, as defined by corporate confidentiality guidelines, details of which can be found in the *Employee Handbook* policies or IT Faculty and Staff Technology handbook. Examples of confidential information include but are not limited to: corporation private, corporate strategies, competitor sensitive, trade secrets, specifications, customer lists, and research data. Employees should take all necessary steps to prevent unauthorized access to this information.
- Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System level passwords should be changed quarterly; user level passwords should be changed every six months.
- All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 15 minutes or less, or by locking your computers manually (Win+L), or logging-off when the host will be unattended.
- Use encryption of information in compliance with CIU's Acceptable Encryption Use policy.
- Because information contained on portable computers is especially vulnerable, special care should be exercised. Protect laptops in accordance with the "Laptop Security Tips". Postings by employees from a CIU email address to news groups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of CIU, unless posting is in the course of business duties.
- All hosts used by the employee that are connected to the CIU *Internet/Intranet/Extranet*, whether owned by the employee or CIU, shall be continually executing approved *virus*scanning *software* with a current *virus* database unless overridden by departmental or group policy.
- Employees must use extreme caution when opening email attachments received from unknown senders, which may contain *viruses*, *email bombs*, or *Trojan horse code*.

Unacceptable Use
The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a website if that website is disrupting production services). Under no circumstances is an employee of CIU authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing CIU-owned resources. The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities:
The following activities are strictly prohibited, with no exceptions:

- Violations of the rights of any person or corporation protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other *software* products that are not appropriately licensed for use by CIU.
- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the

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.

This policy applies to all employees governing their personal *social media* activities as well as their activities that officially represent the organization.

- In the rapidly expanding world of electronic communication, *social media* can mean many things. *Social media* includes all means of communicating or posting information or content of any sort on the Internet, including to your own or someone else's web log or blog, journal or diary, personal web site, social networking or affinity web site, web bulletin board or a chat room, whether or not associated or affiliated with CIU, as well as any other form of electronic communication. As such it includes, *blogging*, instant messaging, emailing, texting, and the use of *social media* such as Facebook, MySpace, LinkedIn, Twitter, Instagram, SnapChat, Google Plus, Pinterest, Match.com, E-harmony, Cupid.com, FlickR, Picasa, Snapfish, Tumblr, Reddit, and other similar sites.
- Ultimately, you are solely responsible for what you post online. Before creating online content, consider some of the risks and rewards that are involved. Any of your online conduct that adversely affects your job performance, the performance of co-workers, or otherwise adversely affects students, prospective students, suppliers, or people who work on behalf of CIU may result in disciplinary action up to and including termination. This would include any postings that contain discriminatory remarks, harassment, and threats of violence or similar inappropriate or unlawful conduct.
- All employees are personally responsible for the content of their online communications. If an employee anticipates having content in his/her communications that identifies, discusses, or provides information about CIU or any of its services, the employee should make it clear that the information and content contained in the communication are the employee's personal views and opinions, and not those of CIU, co-workers, students, suppliers, or people working on behalf of CIU. You should include a disclaimer such as, "The postings on this site are my own and do not necessarily reflect the views of CIU." If you have any questions about the sufficiency of your disclaimer, allow the CIU's Human Resources Director to review your language.
- Employees are not permitted to visit social media sites or blog while at work unless it is for a previously authorized business-related purpose. Do not use a CIU email address to register on social networks, blogs, or other online tools utilized for personal use.
- Do not create a link from your blog, website, or other social networking site to the CIU website without identifying yourself as a CIU associate and using the appropriate disclaimer.
- If you are viewing social media sites for work-related purposes, you should make sure to understand the site's rules for usage and then comply with the same. If you wish to establish a social media site for work related purposes, you must submit your request for a work related social media site to the Marketing Department in accordance with the Marketing Social Media Policy.
- All of CIU's rules and policies regarding the use or communication of CIU's confidential and proprietary information apply to an employee's blog or online communications as well as those created for department related purposes. Discussion of any specific student or prospective student is to be in compliance with the Family Educational Rights and Privacy Act ("FERPA") for higher education students and Gramm-Leach-Bliley Act (GLB) for Ben Lippen students. Both the FERPA and GLB statements can be found in HR Forms webpage on MyCIU.
- CIU expects its employees to use appropriate conduct in the use of their online postings. Never "friend" anyone simply to obtain information that may be helpful. Make sure you are always honest and accurate when posting information or news, and if you make a mistake, correct it quickly. Be open about any previous posts you have altered. Remember that the Internet archives almost everything; therefore, even deleted postings can be searched. Never post any information or rumors that you know to be false about CIU, co-workers, students, prospective students, suppliers, competitors, or people working on behalf of CIU.
- Always be fair and courteous to co-workers, students, prospective students, suppliers, or people who work on behalf of CIU. You are more likely to resolve work-related complaints by speaking directly with your co-workers or the Human Resources Director than by posting complaints to a social media outlet.
- Nevertheless, if you decide to post complaints or criticism, avoid using statements, photographs, video, or audio that reasonably could be viewed as malicious, obscene, threatening or intimidating, or that might constitute harassment or bullying. Examples of such conduct might include offensive posts meant to intentionally harm someone's reputation or posts that could contribute to a hostile work environment on the basis of race, sex, disability, religion or any other status protected by law or company policy.
- Nothing in this policy should be interpreted in a manner that unlawfully prohibits the right of its employees under the National Labor Relations Act or any other law. CIU has and will comply fully with its obligations under federal labor and employment laws.

- CIU prohibits retaliation against any employee for reporting a possible violation of this policy or for cooperating in an investigation.
- Any information communicated in an online posting that violates CIU policies is a serious offense that could lead to disciplinary action, up to and including termination.
- As with all policies, if you have any questions about appropriate postings on your personal online communications, please speak with the Human Resources Director.
- All employees must seek the approval and guidance of Marketing & Communications before establishing any social media accounts to use for the official business purpose and/or marketing of the university, its programs, initiatives, colleges, organizations, departments. See the Marketing Social Media Policy for more information.

Condensed Policy Summary for Login Acknowledgement

Below is condensed version of policy to be used at network login prompt.

- **Network Security** Only authorized users, using CIU registered equipment, are allowed to connect to the CIU network. You are responsible for all activity from your account. As a user, you are responsible for ensuring that others do not use your system privileges. You must take great care to protect your usernames and passwords from eavesdropping or careless misplacement. Your user ID is for your use alone. Passwords are never to be "loaned." No one may use another person's password or access files under a false identity. Allowing others to use your ID or password may result in disciplinary action, including a loss of network login privileges. Student workers requiring network access must be given a network account in their name. If you suspect unauthorized use of your account, notify the IT Services Support Line immediately at X5199.

- **Copyright, File Swapping, and the Law** Except within strict boundaries defined by U.S. Copyright Law, the use of a computer to receive, copy, store, modify or transmit material (e.g. music, movies, *software*, text, photographs, illustrations, material obtained through Internet file-swapping services) without written permission from the copyrighted material's owner is a violation of federal law. According to U.S. Copyright Law, copyright violations can be subject to civil damages of as much as $150,000 per work copied plus additional criminal penalties. Non-adherence to the law could place you and CIU in serious legal jeopardy, opening the institution to significant lawsuits and public embarrassment. Illegal file swapping or any other method of copyright violation is not permitted.

Enforcement:

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Hyperlinks

www.ciu.edu/policy