Acceptable Use Security Policy

1.0 Overview

LeMoyne-Owen College's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to LeMoyne-Owen College's established culture of openness, trust and integrity. LeMoyne-Owen College is committed to protecting LeMoyne-Owen College's employees, customers, partners, and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of LeMoyne-Owen College. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations.

Effective security is a team effort involving the participation and support of every LeMoyne-Owen College employee and affiliate who deals with information and/or information systems.

2.0 Purpose

The purpose of this policy is to outline the acceptable use of computer systems at LeMoyne-Owen College. These rules are in place to protect the employee and LeMoyne-Owen College. Inappropriate use exposes LeMoyne-Owen College to risks including virus attacks, compromise of systems and services, and legal issues.

3.0 Definitions

Term	Definition
Blogging	Writing a blog. A blog (short for weblog) is a personal online journal that is frequently updated and intended for public consumption.
Spam	Unauthorized and/or unsolicited electronic mass mailings.

4.0 Scope

This policy applies to employees, contractors, consultants, temporaries, and other workers at LeMoyne-Owen College, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by LeMoyne-Owen College.

5.0 Policy

5.1 General Use and Ownership

All requests for access to LeMoyne-Owen College networks and systems must be approved by LeMoyne-Owen College IT and the department head.

While LeMoyne-Owen College's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of LeMoyne-Owen College. Because of the need to protect LeMoyne-Owen College's network, management cannot guarantee the confidentiality of information stored on any network device belonging to LeMoyne-Owen College. Employees

Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.

For security and network maintenance purposes, authorized individuals within LeMoyne-Owen College may monitor equipment, systems, and network traffic at any time, per the LeMoyne-Owen College Audit Policy.

Employees and contractors will be removed from access to all LeMoyne-Owen College systems and networks upon the day of termination or earlier.

LeMoyne-Owen College reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

5.2 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 Human Resources policies. Examples of confidential information include but are not limited to: company 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 10 minutes or less, or by logging-off when the host will be unattended. Use encryption of information in compliance with LeMoyne-Owen College's Acceptable Encryption Use Policy.

Because information contained on portable computers is especially vulnerable, special care should be exercised and disk encryption is recommended.

Postings by employees from LeMoyne-Owen College email addresses to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of LeMoyne-Owen College, unless posting is in the course of business duties.

All systems used by the employee that are connected to the LeMoyne-Owen College Internet/Intranet/Extranet, whether owned by the employee or LeMoyne-Owen College, 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 or other malware.

5.3 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 host if that host is disrupting production services).

Under no circumstances is an employee of LeMoyne-Owen College authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing LeMoyne-Owen College-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.

5.3.1 System and Network Activities

The following activities are strictly prohibited:

- Violations of the rights of any person or company 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 LeMoyne-Owen College. 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 LeMoyne-Owen College 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, e-mail 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 LeMoyne-Owen College computing assets to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

- Making fraudulent offers of products, items, or services originating from any LeMoyne-Owen College 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 LeMoyne-Owen College IT 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, LeMoyne-Owen College employees to parties outside LeMoyne-Owen College.

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

5.4 Blogging

Blogging by employees, whether using LeMoyne-Owen College's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of LeMoyne-Owen College's systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate LeMoyne-Owen College's policy, is not detrimental to LeMoyne-Owen College's best interests, and does not interfere with an employee's regular work duties. Blogging from LeMoyne-Owen College's systems is also subject to monitoring.

LeMoyne-Owen College's Confidential Information policy also applies to blogging. As such, Employees are prohibited from revealing any LeMoyne-Owen College confidential or proprietary information, trade secrets or any other material covered by LeMoyne-Owen College's Confidential Information policy when engaged in blogging.

Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of

LeMoyne-Owen College and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by LeMoyne-Owen College's Non-Discrimination and Anti-Harassment policy.

Employees may also not attribute personal statements, opinions or beliefs to LeMoyne-Owen College when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of LeMoyne-Owen College. Employees assume any and all risk associated with blogging.

Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, LeMoyne-Owen College's trademarks, logos and any other LeMoyne-Owen College intellectual property may also not be used in connection with any blogging activity.

6.0 Enforcement

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

Controls

OM4.0 - Organization Approved Browsers and Plugins

Organization approved browsers are used by its members. This includes authorized browser plugins and configurations.

7.0 Revision History

Date of Change	Responsible	Summary of Change
03/16/2020	IT	Updated and converted to new format