LeMoyne-Owen College

IC3 - Internet Usage

March 16, 2020

IC3 - Internet Usage

Organization members use the organization internet connection responsibly and appropriately.

LeMoyne-Owen College
Internet Usage

1.0 Summary

The Internet usage Policy applies to all Internet users (individuals working for the company, including permanent full-time and part-time employees, contract workers, temporary agency workers, business partners, and vendors) who access the Internet.

2.0 Usage Threats

Internet connectivity presents the company with risks that must be addressed to safeguard the facility's vital information assets. These risks include:

2.1 Inappropriate Use of Resources

Access to the Internet by personnel that is inconsistent with business needs results in the misuse of resources. These activities may adversely affect productivity due to excessive time spent using the Internet in ways that are not relevant to the company's business. Additionally, the company may face loss of reputation and possible legal action through other types of misuse.

2.2 Misleading or False Information

All information found on the Internet should be considered suspect until confirmed by another reliable source. There is no quality control process on the Internet, and a considerable amount of its information is outdated or inaccurate.

3.0 Internet Services

Access to the Internet will be provided to users to support business activities and only on an as-needed basis to perform their jobs.

3.1 User Services

3.1.1 Internet Services Allowed

Internet access is to be used for business purposes only. Capabilities for the following standard Internet services will be provided to users as needed:

- Email and IM: Send/receive messages to/from the Internet (with or without document attachments).
- Web Navigation: Browsing as necessary for business purposes, using a hypertext transfer protocol (HTTP) browser. Full access to the Internet; limited access from the Internet to dedicated company public web servers only.
- File Sharing and File Transfer Protocol (FTP): Send data/files and receive inbound data/files, as necessary for business purposes.

Management reserves the right to add or delete services as business needs change or conditions warrant. All other services will be considered unauthorized access to/from the Internet and will not be allowed.

3.2 Request & Approval Procedures

Internet access will be provided to users to support business activities and only as needed to perform their jobs.

3.2.1 Request for Internet Access

Requests must be made through LeMoyne-Owen College IT for users who require internet access to perform their jobs.

3.2.2 Approval

Approval is required through LeMoyne-Owen College IT for users who require internet access to perform their jobs.

3.2.3 Removal of Privileges

Internet access will be discontinued upon termination of employee, completion of contract, end of service of non-employee, or disciplinary action arising from violation of this policy. In the case of a change in job function and/or transfer the original access code will be discontinued, and only reissued if necessary and a new request for access is approved.

All user IDs that have been inactive for thirty (30) days will be revoked. The privileges granted to users must be reevaluated by management annually. In response to feedback from management, systems administrators must promptly revoke all privileges no longer needed by users.

4.0 Usage Policies

4.1 Resource Usage

Access to the Internet will be approved and provided only if reasonable business needs are identified. Internet services will be granted based on an employee's current job responsibilities. If an employee moves to another business unit or changes job functions, a new Internet access request must be submitted within 5 days.

User Internet access requirements will be reviewed periodically by company departments to ensure that continuing needs exist.

4.2 Allowed Usage

Internet usage is granted for the sole purpose of supporting business activities necessary to carry out job functions. All users must follow the corporate principles regarding resource usage and exercise good judgment in using the Internet.

Acceptable use of the Internet for performing job functions might include:

- Web applications for business and limited personal purposes.
- Communication between employees and non-employees for business purposes
- IT technical support downloading software upgrades and patches
- Review of possible vendor web sites for product information
- Reference regulatory or technical information
- Research

4.3 Personal Usage

Using company computer resources to access the Internet for personal purposes beyond a reasonable amount, without approval from the user's manager and LeMoyne-Owen College IT, may be considered cause for disciplinary action up to and including termination.

All users of the Internet should be aware that the company network creates an audit log reflecting request for service, both inbound and outbound addresses, and is periodically reviewed.

Users who choose to store or transmit personal information such as private keys, credit card numbers or certificates or make use of Internet "wallets" do so at their own risk. The company is not responsible for any loss

of information, such as information stored in the wallet, or any consequential loss of personal property.

4.4 Prohibited Usage

Acquisition, storage, and dissemination of data which is illegal, pornographic, or which negatively depicts race, sex or creed is specifically prohibited.

The company also prohibits the conduct of a business enterprise, political activity, engaging in any form of intelligence collection from our facilities, engaging in fraudulent activities, or knowingly disseminating false or otherwise libelous materials.

Other activities that are strictly prohibited include, but are not limited to:

- Accessing company information that is not within the scope of one's work. This includes unauthorized reading of customer account information, unauthorized access of personnel file information, and accessing information that is not needed for the proper execution of job functions.
- Misusing, disclosing without proper authorization, or altering customer or personnel information. This includes making unauthorized changes to a personnel file or sharing electronic customer or personnel data with unauthorized personnel.
- Deliberate pointing or linking of company Web sites to other internet sites whose content may be inconsistent with or in violation of the aims or policies of the company.
- Any conduct that would constitute or encourage a criminal offense, lead to civil liability, or otherwise violate any regulations, local, state, national or international law including without limitations US export control laws and regulations.
- Use, transmission, duplication, or voluntary receipt of material that infringes on the copyrights, trademarks, trade secrets, or patent rights of any person or organization. Assume that all materials on the Internet are copyright and/or patented unless specific notices state otherwise.
- Transmission of any proprietary, confidential, or otherwise sensitive information without the proper controls.
- Creation of, posting, transmission, or voluntary receipt of unlawful, libelous, offensive, threatening, harassing material, including but not limited to comments based on race, national origin, sex, sexual orientation, age, disability, religion, or political beliefs.
- Any form of gambling.

Unless specifically authorized under the provisions of section 4.3, the following activities are also strictly prohibited:

- Unauthorized downloading of any shareware programs or files for use without authorization in advance from LeMoyne-Owen College IT and the user's manager.
- Playing of any games.
- Forwarding of chain letters.
- Participation in any online contest or promotion.
- Acceptance of promotional gifts.

Bandwidth both within the company and in connecting to the Internet is a shared, finite resource. Users must make reasonable efforts to use this resource in ways that do not negatively affect other employees. Specific departments may set guidelines on bandwidth use and resource allocation, and may ban the downloading of particular file types.

4.5 Software Licenses

The company supports strict adherence to software vendor license agreements. When at work or when company computing or networking resources are used, copying of software in a manner inconsistent with the vendor's license is forbidden. Questions regarding lawful versus unlawful copying should be referred to LeMoyne-Owen College IT for review or to request a ruling from the Legal Department before any duplication is done.

Similarly, reproduction of materials available over the Internet must be done only with the written permission of the author or owner of the document. Unless permission from the copyright owner(s) is first obtained, making copies of material from magazines, journals, newsletters, other publications and online documents is forbidden unless this is both reasonable and customary. This notion of "fair use" is in keeping with international copyright laws.

4.6 Review of Public Information

All publicly-writable directories on Internet-connected computers may be reviewed and cleared each evening. This process is necessary to prevent the anonymous exchange of information inconsistent with company business. Examples of unauthorized public information include pirated information, passwords, credit card numbers, and pornography.

4.7 Expectation of Privacy

4.7.1 Monitoring

Users should consider their Internet activities as periodically monitored and limit their activities accordingly.

Management reserves the right to examine email, personal file directories, web access, and other information stored on company computers, at any time and without notice. This examination ensures compliance with internal policies and assists with the management of company information systems.

4.7.2 Email Confidentiality

Users should be aware that clear text email is not a confidential means of communication. The company cannot guarantee that electronic communications will be private. Employees should be aware that electronic communications can, depending on the technology, be forwarded, intercepted, printed, and stored by others. Users should also be aware that once an email message is transmitted it may be altered. Deleting an email from an individual workstation will not eliminate it from the various systems across which it has been transmitted.

4.8 Maintaining Corporate Image and Goodwill

4.8.1 Representation

When using company resources to access and use the Internet users must realize they represent the company. Whenever employees state an affiliation to the company they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the company".

4.8.2 Company Materials

Users must not place company material (examples: internal memos, press releases, product or usage information, documentation, etc.) on any mailing list, social media service, or such service. Any posting of materials must be approved by the employee's manager and the public relations department and will be placed by an authorized individual.

4.8.3 Creating Web Sites

All individuals and/or business units wishing to establish an external web page or site must first develop business, implementation, and maintenance plans. Formal authorization must be obtained through LeMoyne-Owen College IT. This will maintain publishing and content standards needed to ensure consistency and appropriateness.

In addition, contents of the material made available to the public through the Internet must be formally reviewed and approved before being published. All material should be submitted to the LeMoyne-Owen College Corporate Marketing team for initial approval to continue. All company pages are owned by, and are the ultimate responsibility of LeMoyne-Owen College Marketing.

All company web sites must be protected from unwanted intrusion through formal security measures which can be obtained from LeMoyne-Owen College IT.

4.9 Periodic Reviews

4.9.1 Usage Compliance Reviews

To ensure compliance with this policy, periodic reviews will be conducted. These reviews will include testing the degree of compliance with usage policies.

4.9.2 Policy Maintenance Reviews

Periodic reviews will be conducted to ensure the appropriateness and the effectiveness of usage policies. These reviews may result in the modification, addition, or deletion of usage policies to better suit company information needs.

5.0 Enforcement

Violations of the LeMoyne-Owen College Internet usage Policy can lead to revocation of system privileges and/or disciplinary action up to and including termination. Additionally, the company may at its discretion seek legal remedies for damages incurred as a result of any violation.

Controls

IC3.0 - Network Data Loss Prevention

File Data Loss Prevention (DLP) solution protects confidential/sensitive information in the corporate environment.

IC3.1 - Internet Content Monitoring

Internet content is monitored with employee knowledge.