THE LeMoyne-Owen COLLEGE

LEADERSHIP. OPPORTUNITY. CHANGE.

LeMoyne-Owen College

IC4 - Information Security/Sensitivity

March 16, 2020

IC4 - Information Security/Sensitivity

The organization understands how to determine what information is sensitive and how to handle each level of sensitive information. This includes public, company confidential and 3rd party confidential information.

LeMoyne-Owen College Information Security/Sensitivity

1.0 Purpose

LeMoyne-Owen College maintains a strong commitment to information security. This Information Security/Sensitivity Policy is intended to help employees determine what information can be disclosed to non-employees, as well as the relative sensitivity of information that should not be disclosed outside of LeMoyne-Owen College without proper authorization.

The information covered in these guidelines includes, but is not limited to, information that is either stored or shared via any means. This includes: electronic information, information on paper, and information shared orally or visually (such as telephone and video conferencing).

All employees should familiarize themselves with the information labeling and handling guidelines that follow this section. It should be noted that the sensitivity level definitions were created as guidelines and to emphasize common sense steps that you can take to protect LeMoyne-Owen College Confidential information (e.g., LeMoyne-Owen College Confidential information should not be left unattended in conference rooms).

Note: The impact of these guidelines on daily activity should be minimal.

2.0 Scope

This policy applies to employees, contractors, consultants, temporaries and third-party affiliates.

LeMoyne-Owen College personnel are encouraged to use common sense judgment in securing LeMoyne-Owen College Confidential information to the proper extent. If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact their manager or IT.

3.0 Policy

3.1 Data Classification Levels

The Sensitivity Guidelines below provides details on how to protect information at varying sensitivity levels. Use these guidelines as a reference only, as LeMoyne-Owen College Confidential information in each column may necessitate more or less stringent measures of protection depending upon the circumstances and the nature of the LeMoyne-Owen College Confidential information in question.

Level 1: Confidential Requiring Notification

Confidential Requiring Notification data includes any information that LeMoyne-Owen College has a contractual, legal or regulatory obligation to safeguard in the most stringent manner. In some cases, unauthorized disclosure or loss of this data would require the company to notify the affected individual and state or federal authorities. In some cases, modification of the data would require informing the affected individual.

The company's obligations will depend on the particular data and the relevant contract or laws. Systems and processes protecting the following types of data need to meet that baseline:

- Personally identifiable health information that is not subject to HIPAA.
- Personally Identifiable Information (PII) covered under Massachusetts General Law chapter 93H and 201 CMR 17, including an individual's name plus the individual's Social Security Number, driver's license number, or financial account number.

- Personal Data covered under the European General Data Protection Regulation (GDPR).
- Personal Data covered under the California Consumer Privacy Act as of January 1, 2020.
- "Criminal Background Data" that might be collected as part of an application form or a background check.

More stringent requirements exist for some types of Confidential Requiring Notification data. Individuals working with the following types of data must follow the company policies governing those types of data and consult with **IT and Department Heads** to ensure they meet all of the requirements of their data type:

- Cardholder and transaction data subject to Payment Card Industry Data Security Standard (PCI-DSS) which sets the standards for security of credit, debit and cash card transactions.
- Protected Health Information (PHI) subject to the Health Insurance Portability and Accountability Act (HIPAA), which sets standards for protection of medical records and patient data. See the HIPAA Policy for details.
- Controlled Unclassified Information required to be compliant with NIST 800.171.
- Data controlled by U.S. Export Control Law such as the International Traffic in Arms Regulations (ITAR) or Export Administration Regulations (EAR). ITAR and EAR have additional requirements.
- U.S. Government Classified Data.
- Restricted Use data should be used only when no alternative exists and must be carefully protected. Any unauthorized disclosure, unauthorized modification, or loss of Restricted Use data must be reported to the Information Security Team.

Contractual obligations to other firms must be addressed on per company basis depending on what was agreed.

Level 2: Confidential

Confidential data is information that is proprietary in nature and should not be disclosed to others. This information should be protected against unauthorized disclosure or modification. Confidential data should be used only when necessary for business purposes and should be protected both when it is in use and when it is being stored or transported.

Examples of Internal data include: Internal correspondence, planning documents, technical specifications, product code and meeting minutes; contact lists that contain information that is not publicly available; and procedure documentation that should remain private. Passwords, Private Keys and System Keys are a special type of Level 2 data. Any unauthorized disclosure or loss of Confidential data must be reported to the **IT/Information Security Team**.

Level 3: Unrestricted

Unrestricted data is public data information that may be disclosed to any person regardless of their affiliation with the company. The Unrestricted classification is not limited to data that is of public interest or intended to be distributed to the public; the classification applies to data that do not require any level of protection from disclosure. While it may be necessary to protect original (source) documents from unauthorized modification, Public data may be shared with a broad audience both within and outside the company, and no steps need be taken to prevent its distribution.

Examples of Unrestricted data include: press releases, directory information, application and request forms, and other general information that is openly shared.

3.2 Data Protection Standards

Each classification of data has different requirements for protection throughout the lifecycle of use.

Users are expected to use good judgement, in case of any uncertainty about classification level of any data, the Information Security Team should assist in making the decision.

Collection

- Collection of Level 1 data about individuals must be approved by the Information Security Team.
- Reduce or eliminate collection of Level 1 and Level 2 data when not required for business functions.
- There are no restrictions on collection of Level 3 data.

Access

- Access to Level 1 and Level 2 data requires approval of the Information Security Team.
- Avoid accessing or using Level 1 data whenever possible and do so from as few different devices as

possible. Restricted information access must be immediately removed from any person that no longer requires that access as part of their job function.
- Access to Level 2 data should be provided as required for business devices used to access sensitive (non-Public) information and decides must meet minimum security standards.

Sharing

- If you are uncertain if a piece of Level 1 information should be shared, escalate the request to the Information Security Team. This information may be shared only for need-to-know business purposes and only as approved.
- Note: Non-disclosure and other types of agreements (business associate agreements) may be necessary. Such agreements or agreement forms must be approved by **Department Heads.**
- In case of uncertainty of the confidentiality of a piece of data, escalate the request to the Information Security Team. Information may be shared only for business purposes.
- Level 2 data can be shared with employees as needed and shared with vendors/third-parties as approved by the department head.

Auditing

Each unit or department must conduct periodic reviews of where Level 1 and Level 2 data is located, who has access to it, the access control mechanisms, encryption protocols, and data destruction protocols. Verify that procedures for removing access are documented and accurate.

Incident Reporting

Any unauthorized disclosure or loss of Level 1 or Level 2 information must be reported to the Information Security Team.

Storage

Individual access controls are required for electronic information. Physical security is generally used, and information shall be stored in a physically secured computer. Level 1 data must be stored in an encrypted manner. Acceptable Encryption policy provides standards for encryption of data at rest. Inventories of Level 1 and Level 2 data and the LeMoyne-Owen College system used for said information must be maintained.

Data Retention

- Emails shall be retained for a period of two months after which they shall be archived.
- Data shall be retained for [*insert specific period of time, or suggest stating "as long as is necessary to provide the service to the client."*] After the retention period is over or upon specific request by the client, data shall be destroyed in accordance with Destruction and Disposal defined in this policy.

Destruction and Disposal

The IT department maintains and shall enforce a detailed list of approved destruction methods appropriate for each type of information stored, whether in physical storage media or in database records or backup files. When systems containing data are decommissioned, they must follow the following destruction policy:

- Paper documents containing Level 1, Level 2 information shall be shredded using secure, locked consoles designated in each office from which waste shall be periodically picked up by a security screened personnel.
- Level 1 and Level 2 information on electronic files and data on Reusable Electronic Storage Devices should be reliably erase or physically destroy media using DOD Standard for Secure Data Sanitation (DOD 5220.22M). Functional electronic media that can be overwritten using a secure erase tool then may be recycled or disposed of. Non-functional electronic media (damaged disk drives) must be physically destroyed.
- Devices such as Printers, Copiers, Multifunction office machines often contain hard drives which must be properly erased, or "wiped", prior to leaving LeMoyne-Owen College control (returned to the vendor, sent to surplus, donated, disposed of, etc.).

Do not destroy records that are the subject of a litigation hold or that must be retained.

The specific deletion or destruction process may be carried out either by an employee or internal/external service providers. All external service providers must be thoroughly vetted and reviewed to ensure their full compliance with data protection requirements, and all data disposal is subject to applicable provisions under

relevant data protection laws.

Unless specified, no controls are required for Level 3 data.

4.0 Customer Information Handling

All customer information is treated as Level 1 data and should be handled in accordance with this policy. All workstations accessing customer information must follow LeMoyne-Owen College **Workstation Security Policy** at all times.

Customer information shall be retained as per the customer agreement or for as long as it is required for it's understood purpose.

Data Retention

Customer data will be retained only for as long as **LeMoyne-Owen College** needs it to fulfil the purpose for which data has been collected. Customers can submit data deletion requests in case of termination, cancellation, expiration or other conclusion of the agreement. Data shall be deleted within 30 days of a data deletion requests.

Security Review

LeMoyne-Owen College may provide customers with the right to review LeMoyne-Owen College's security controls annually for the entire period that LeMoyne-Owen College processes, stores or otherwise has access to Customer Confidential Information. LeMoyne-Owen College may provide customers with access to independent audit reports that have been performed on LeMoyne-Owen College. If issues are found during a customer review of LeMoyne-Owen College's security controls, LeMoyne-Owen College will file a remediation plan with the customer within thirty (30) days following the completion of such a review, and LeMoyne-Owen College will remediate each such issue in a timely manner in accordance with a remediation schedule agreed to by the parties.

Security Incidents

LeMoyne-Owen College shall notify customers of any information security breach involving Customer Confidential Information, including any security breach at or involving a Contractor's systems, hardware, equipment, devices or premises computers or otherwise involving a Contractor's personnel; LeMoyne-Owen College shall provide notification of any such incident promptly, but in no event later than seven (7) days (or if such incident involves Customer's Sensitive Information, in no event later than three (3) days) following the date LeMoyne-Owen College first becomes aware of such an incident.

Application Vulnerabilities

LeMoyne-Owen College shall notify customers of any high-risk vulnerabilities or defects found within products or services within 72 hours of remediation of those defects. LeMoyne-Owen College

5.0 Exceptions and Enforcement

CEO/IT is authorized to grant exceptions to the requirements set forth in this document. Requests for exceptions shall be initiated through a *request email, ticket, etc.* Any exception granted will require a thorough review of the situation and will be based on the implementation of appropriate compensating controls.

Some data may be subject to specific protection requirements under a contract or grant, or according to a law or regulation not described here, in those circumstances, the most restrictive protection requirement should apply.

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

Penalty for deliberate or inadvertent disclosure: Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

Controls

IC4.0 - Information Classification

Information is classified and labeled in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification.

IC4.10 - Data Collection Consent

The organization gets explicit consent from data subjects (customers, consumers, website visitors, employees, etc.) before collecting private information.

IC4.11 - Private Data Requests

The organization responds to data management (viewing, deletion, correction) requests from data subjects.

IC4.12 - Private Data Retention

The organization may only keep and process private data for as long as is required for it's understood purpose.

IC4.13 - Limited Use and Disclosure of PHI

The organization exercises reasonable efforts to use, disclose, and request only the minimum amount of protected health information needed to accomplish the intended purpose of the use, disclosure, or request.

IC4.14 - Define Data for Processing Integrity

Define a complete list of what data is processed as part of your product or service, and how processing integrity is measured.

IC4.15 - Information in Non-Production Systems

The organization does not permit the use and storage of confidential information (as defined in IC4 - Information Security/Sensitivity policy) in non-production systems and environments.

IC4.1 - Information Labelling

Information is labeled in accordance with the information classification scheme adopted by the organization.

IC4.2 - Information Management

Assets are handled in accordance with the information classification scheme adopted by the organization.

IC4.3 - Information Protection in Transit

Application information passing over public networks are encrypted to protect it from fraudulent activity, contract disputes and unauthorized disclosure and modification.

IC4.4 - Information Acceptable Use

Rules for the acceptable use of information and of assets associated with information and information processing facilities are identified, documented and implemented.

IC4.5 - Information Protection at Rest

Sensitive data is encrypted at rest to protect the integrity of the information.

IC4.6 - Data Entry Validation

An input validation system setting that ensures data entry fields are entered correctly

IC4.7 - Hardcopy Document Disposal

Printed materials containing sensitive customer information are disposed of securely.

IC4.8 - Data Privacy Officer

The organization has a designated Data Privacy Officer (DPO)

IC4.9 - Privacy Policy Statement

The organization has a privacy statement describing privacy (GDPR, etc.) commitments in accordance to local laws and regulations.