

**LOUISIANA COMMUNITY & TECHNICAL COLLEGE SYSTEM**  
**Internal Policy**

**Title: Information Security and Acceptable Use Policy (ISAP)**

<b>Authority:</b> System President	Original Adoption: Feb. 08, 2018
	Effective Date: Feb. 08, 2018
	Last Revision: Feb. 08, 2018

**Policy Statement**

All Louisiana Community and Technical College (LCTCS) Board Office employees and third parties that create, use, maintain or handle LCTCS IT resources shall follow LCTCS’s Information Security and Acceptable Use Policy (ISAP). All Louisiana Community and Technical College (LCTCS) Board Office Information Technology (IT) resources shall only be used to support the administrative needs of the LCTCS Board Office. This policy applies to employees of the Louisiana Community and Technical College System (LCTCS) Board Office, contractors and vendors that connect to servers, applications or network devices that contain or transmit LCTCS Protected Data.

This policy shall be subject to and superseded by applicable regulations and laws.

**Policy Purpose**

The Information Security and Acceptable Use Policy applies to all users of LCTCS Board Office IT resources. The purpose of the LCTCS Board Office IT resources is to support the administrative needs of the college system. LCTCS has a responsibility to ensure that IT resources be used in a manner that supports the business needs of the Board Office, and that protects the institution from harm that may result from misuse. Accordingly, the ISAP supports the following goals:

1. Promote a “security is everyone’s responsibility” philosophy to assist the LCTCS Board Office in meeting its business and legal commitments.
2. Ensure that the LCTCS Board Office complies with all applicable laws and regulations.
3. Ensure the integrity, reliability, availability and superior performance of IT resources.
4. Ensure that users are protected from data breach and cybercrime.
5. Prevent unauthorized disclosure of critical information.
6. Ensure the LCTCS Board Office is protected from financial, legal, regulatory and reputational harm.
7. Ensure that IT systems are used for their intended purposes.
8. Establish processes for addressing policy violations and sanctions for violators.

**Policy Violation**

1. Violation of the ISAP may result in disciplinary action, up to and including termination of employment.

2. The LCTCS Board Office reserves the right to report violations of federal, state and local laws and regulations governing computer and network use, as well as interactions that occur on the Internet, to authorities as deemed appropriate.
3. Users who violate the ISAP may be held liable for damages to LCTCS Board Office assets, including but not limited to the loss of information, computer software and hardware, lost revenue due to down time, fines and judgments imposed as a direct result of the violation.
4. The LCTCS Board Office reserves the right to deactivate a user's access rights, whether or not the user is suspected of any violation of this policy, when necessary to preserve the integrity of IT Resources.

## **Policy Exceptions**

Policy exceptions to the LCTCS Board Office Information Security policy will be permitted only when approved in advance and in writing by the LCTCS System President.

### **I. Information Security**

#### **General Use and Responsibilities:**

1. Maintain current knowledge of, and comply with, the contents of the ISAP.
2. Distribute confidential and sensitive information on a limited basis to those with a business need to know the information.
3. Protect all PII, NPI, PCI and other regulated or proprietary data from unauthorized access.
4. Notify the IT Department and/or the IT Helpdesk of any suspected breaches.

### **II. Acceptable Use**

#### **General Use and Responsibilities:**

The ISAP establishes specific requirements for the use of LCTCS Board Office IT resources by any user, including those used in connection with a privately owned computer or other device. The LCTCS Board Office reserves the right to amend or otherwise revise this document as necessary. Users are responsible for reviewing the ISAP periodically to ensure continued compliance. By using IT resources, the user agrees to the terms and conditions of the ISAP. Users consent to the LCTCS Board office's use of scanning programs for security purposes on privately owned computers or other devices while they are attached to the LCTCS network.

1. All computing and mobile devices that connect to the LCTCS network are subject to the ISAP.
2. Users include, but are not limited to, all LCTCS employees, contractors, guests, consultants, and other workers, including all personnel affiliated with third parties.
3. Users shall access only IT resources for which they have authorization.

4. Users are individually responsible for appropriate use of their computer, account and the IT resources assigned to them.
5. Users have a responsibility to report the theft, loss or unauthorized disclosure of LCTCS Board Office proprietary information and/or IT resources.
6. Users shall not use IT resources for uses that are inconsistent, incompatible or in conflict with state or federal law or other LCTCS policies.
7. Users are responsible for exercising good judgment regarding the reasonableness of personal use.
8. The LCTCS Board Office is bound by its contractual and license agreements respecting certain third party software – users are expected to comply with all such agreements when using IT resources.
9. Users shall not intentionally disrupt the computing environment or obstruct the work of other users.

### **III. Access Control**

#### **General Use and Responsibilities:**

These access controls are designed to minimize potential exposure to the LCTCS Board Office resulting from unauthorized use of resources and to preserve and protect the confidentiality, integrity and availability of the System's networks, systems and applications.

This policy applies to employees of the Louisiana Community and Technical College System (LCTCS) Board Office, contractors and vendors that connect to servers, applications or network devices that contain or transmit LCTCS Protected Data.

#### **Policies & Procedures:**

##### **A. User Access**

All users of LCTCS Board Office IT resources will abide by the following set of rules:

- Users with access to LCTCS Board Office IT resources will utilize a unique LCTCS Active Directory (AD) account. This account will conform to the following standards through controls in AD Group Policy:
  - The password will conform, at a minimum, to 12 characters, and must contain 3 of the following 4 characteristics:
    - Upper case letters
    - Lower case letters
    - Numbers
    - Special Characters

- Accounts will require a password change every 105 days
  - Student accounts are not be required to change passwords. However, password strength will be enforced if they change their password (i.e. forgot password).
- Accounts will be locked for no less than 30 minutes upon five unsuccessful login attempts.
- LCTCS Board Office computers will automatically enable the computers screen saver if their session is idle for more than 15 minutes. Re-entry of their password is required to unlock the screen saver.
- LCTCS Board Office computers shall contain a login banner that displays the following content:
 

“This computer system is the property of the Louisiana Community and Technical College System and may be accessed only by authorized users. Unauthorized use of this system is strictly prohibited and may be subject to criminal prosecution. LCTCS may monitor any activity or communication on the system and retrieve any information stored within the system. By accessing and using this computer, you are consenting to such monitoring and information retrieval for law enforcement and other purposes. Users should have no expectation of privacy as to any communication on or information stored within the system, including information stored locally on the hard drive or other media in use with this unit (e.g., floppy disks, PDAs and other hand-held peripherals, CD-ROMs, etc.)”
- Account activity will be logged and monitored.
- Users will not login using generic, shared or service accounts.
- Service providers with remote access to customer premises (for example, for support of systems or servers) must use a unique authentication credential assigned by LCTCS IT.

## **B. Administrative Access**

- IT employees will abide by the above user access guidelines.
- Administrators will immediately revoke all of a user’s access to the LCTCS Board Office network when a change in employment status dictates the user no longer requires such access.
- All service accounts must be used by no more than one service, application, or system.

- Administrators must not extend a user group's permissions in such a way that it provides inappropriate access to any user in that group.

### **C. Remote Access**

All LCTCS Board Office employees accessing LCTCS IT resources remotely must abide by the following rules:

- No non LCTCS Board Office IT network devices are allowed on the LCTCS network, or other unapproved remote access technology.
- All remote access must be authenticated and encrypted through the LCTCS Board Office remote access portal.
- The CIO or their designee must approve all third party access to the LCTCS Board Office network.
- Third parties may access only the systems that they support or maintain.
- All third party accounts in the LCTCS Board Office Active Directory will be disabled and inactive unless needed for support or maintenance. All third parties with access to the LCTCS Board Office network must adhere to all regulations and governance standards associated with that data (e.g. PCI security requirements for cardholder data, FERPA requirements for student records, HIPAA requirements for Protected Health Information). Third party accounts must be immediately disabled after support or maintenance is complete.
- Copying classified and restricted data from LCTCS Board office systems to a user's personal computing device is prohibited.
- Remote access will be disconnected automatically after 8 hours.

### **D. Physical Access**

#### **1. Facilities Security**

- The main entrance to the LCTCS Board Administrative building will be unlocked during regular business hours.
- The main entrance to the LCTCS SIS building will only be unlocked during scheduled meeting and/or training events.
- All other LCTCS Board Office entrances will be secured with access controlled by the LCTCS Board Office building access control system.

- Employees will be granted access right to only those entrances required for the execution of their assigned duties.

## 2. Data Center Security

The LCTCS data center will abide by the following physical security requirements:

- Video surveillance is installed to monitor access into and out of the LCTCS data center.
- Access to the LCTCS data center is controlled using an electronic badge and personal PIN systems. IT staff have badges with security access and require entry of a Personal PIN to gain entry.
  - Only the Director of Facilities, Chief Operations Officer (COO) and Chief Information Officer (CIO) will have physical keys with access to this space.
- Physical access to the LCTCS data center is limited to LCTCS IT Staff or contractors whose job function or responsibilities require such physical access.
- Authorized LCTCS personnel will accompany visitors accessing the LCTCS data center, and all access will be logged via the Data Center Visitor Access Log.
  - This log will be stored in the LCTCS Data Center.
  - Each visitor, and accompanying authorized LCTCS personnel, must sign in and out of the data center.
  - The log data will be kept for at least a period of three months.
- Modification, additions or deletions of physical access to the LCTCS data center will be managed by the CIO.
- All terminated onsite personnel and expired visitor identification (such as ID badges)" will have their access revoked immediately.
- Physical access requires the approval of the Director of Facilities and CIO.
- The CIO will review audit physical access to LCTCS data center on an annual basis.

## 3. Data Closet Security

All data closets in LCTCS Board Office facilities will be secured, and access controlled by employee badge/fob. LCTCS IT Systems Operation and Network

Operations staff will have access granted through the LCTS Board Office building access control system. Access will be restricted to only the Director of Facilities, COO, CIO and aforementioned IT staff will have access.

#### **IV. Data Classification**

##### General Use and Responsibilities:

1. Information Technologies (IT) Responsibility—All IT employees who come into contact with sensitive Louisiana Community and Technical College System (LCTCS) Board Office information are expected to familiarize themselves with this data classification policy and to consistently use these same ideas in their daily LCTCS business activities. Sensitive information is either Confidential or Restricted information, and both are defined later in this document. Although this policy provides overall guidance, to achieve consistent information protection, LCTCS IT employees are expected to apply and extend these concepts to fit the needs of day-to-day operations. This document provides a conceptual model for LCTCS IT for classifying information based on its sensitivity, and an overview of the required approaches to protect information based on these same sensitivity classifications.
2. Addresses Major Risks - The IT data classification system, as defined in this document, is based on the concept of need to know. This term means that information is not disclosed to any person who does not have a legitimate and demonstrable business need to receive the information. This concept, when combined with the policies defined in this document, will protect LCTCS information from unauthorized disclosure, use, modification, and deletion.
3. Applicable Information - This data classification policy is applicable to all electronic information for which LCTCS IT is the custodian.

##### **A. Access Control**

1. Need to Know—Each of the policy requirements set forth in this document are based on the concept of need to know. If an LCTCS IT employee is unclear how the requirements set forth in this policy should be applied to any particular circumstance, he or she must conservatively apply the need to know concept. That is to say that information must be disclosed only to those people who have a legitimate business need for the information.
2. System Access Controls—The proper controls shall be in place to authenticate the identity of users and to validate each user's authorization before allowing the user to access information or services on the system. Data used for authentication shall be protected from unauthorized access. Controls shall be in place to ensure that only personnel with the proper authorization and a need to know are granted access to LCTCS Board office systems and their resources. Remote access shall be encrypted and controlled through identification and authentication mechanisms.

3. Access Granting Decisions—Access to LCTCS Board Office sensitive information must be provided only after the written authorization of the data owner has been obtained. Access requests will be presented to the data owner using the Access Request template. Custodians of the involved information must refer all requests for access to the relevant owners or their delegates. Special needs for other access privileges will be dealt with on a request-by-request basis. The list of individuals with access to Confidential or Restricted data must be reviewed for accuracy by the relevant data owner in accordance with a system review schedule approved by the CIO.

## **B. Information Classification**

1. Owners and Production Information—All electronic information managed by LCTCS IT must have a designated owner. Production information is information routinely used to accomplish business objectives. Owners should be at the Director level or above. Owners are responsible for assigning appropriate sensitivity classifications as defined below. Owners do not legally own the information entrusted to their care. They are instead designated members of the LCTCS management team who act as stewards, and who supervise the ways in which certain types of information are used and protected.

2. CONFIDENTIAL - This classification applies to the most sensitive business information, such as Personally Identifiable Information (PII), that is intended for use strictly within LCTCS. Its unauthorized disclosure could seriously and adversely impact LCTCS, its customers, its business partners, and its suppliers.

3. PRIVATE - This classification applies to less-sensitive business information, such as Non-Public Information (NPI), that is intended for use within LCTCS. Its unauthorized disclosure could adversely impact LCTCS or its customers, suppliers, business partners, or employees.

4. PUBLIC - This classification applies to information that has been identified by LCTCS management as not harmful if disseminated to the public. By definition, there is no such thing as unauthorized disclosure of this information and it may be disseminated without potential harm.

5. Owners and Access Decisions - Data owners must make decisions about who will be permitted to gain access to information, and the uses to which this information will be put. IT must take steps to ensure that appropriate controls are utilized in the storage, handling, distribution, and regular usage of electronic information.

## **C. Object Reuse and Disposal**

Storage media containing sensitive (i.e. restricted or confidential) information shall be completely empty before reassigning that medium to a different user or disposing of it when no longer used. Simply deleting the data from the media is not sufficient. A method must be used that completely erases all data. When disposing of media containing data that cannot be completely erased it must be destroyed in a manner approved by the CIO.



## **D. Special Considerations for Restricted Information**

If restricted information is going to be stored on a personal computer, portable computer, personal digital assistant, or any other single-user system, the system must conform to access control safeguards approved by IT and LCTCS senior management. When these users are not currently accessing or otherwise actively using the restricted information on such a machine, they must not leave the machine without logging off, invoking a password protected screen saver, or otherwise restricting access to the restricted information.

Data Encryption Software – LCTCS employees and vendors must not install encryption software to encrypt files or folders without the express written consent of the CIO.

## **E. Information Transfer**

1. Transmission Over Networks—If LCTCS sensitive data is to be transmitted over any external communication network, it must be sent only in encrypted form. Sensitive data should never be sent in the body of an email and only via encrypted file attachments. The preferred method of dissemination is moving the data to a shared system that requires encryption in transit, encryption at rest, and secure login for the recipient to retrieve (i.e. SharePoint, OneDrive, DropBox)

2. Transfer To Another Computer—Before any sensitive information may be transferred from one computer to another, the person making the transfer must ensure that access controls on the destination computer are commensurate with access controls on the originating computer. If comparable security cannot be provided with the destination system's access controls, then the information must not be transferred.

## **V. Incidence Response**

### General Use and Responsibilities:

All Incident Response plans and procedures shall be documented and implemented to address all incident detections and responses, especially related to critical systems. Louisiana Community and Technical College System (LCTCS) board office staff shall be aware of their responsibilities in detecting security incidents to facilitate the incident response plan and procedures. As part of the organization's communication strategy, incident reports will be sent to the Chief Information Officer (CIO) & Chief Operations Officer (COO).

All incident detections and responses, especially those related to critical systems, shall follow this policy. These processes and procedures exist to mitigate risk, reduce costs, and reduce downtime due to security incidents.

## Policies & Procedures:

### **A. Incident Identification**

1. LCTCS Board Office employees shall be aware of their responsibilities in detecting security incidents to facilitate the incident response plan and procedures.
2. All LCTCS Board Office employees have the responsibility to assist in incident response procedures within their particular areas of responsibility.
3. Some examples of security incidents that an employee might recognize in their day-to-day activities include, but are not limited to:
  - a. Theft, damage or unauthorized access (e.g., unauthorized logins, papers missing from their desk, broken locks, missing log files, an alert from a Public Safety employee, video evidence of a break-in or unscheduled/unauthorized physical entry);
  - b. Fraud (e.g., inaccurate information within databases, logs, files or paper records);
  - c. Abnormal system behavior (e.g., unscheduled system reboot, unexpected messages, abnormal errors in system log files or on terminals);
  - d. Security event notifications (e.g., file integrity alerts, intrusion detection alarms, and physical security alarms).
4. All LCTCS Board Office employees, regardless of job responsibilities, should be aware of the potential incident identifiers and know whom to notify in these situations. In all cases, employee should report incidents per the instructions under Reporting and Incident Declaration below.

### **B. Reporting and Incident Declaration**

1. The CIO shall be notified immediately of any suspected or confirmed security incidents involving LCTCS Board Office computing assets, particularly any critical system(s).
2. If it is unclear whether a situation should be considered a security incident, the CIO should be contacted to evaluate the situation.
3. As part of the organization's communication strategy, incident reports will be forwarded to the CIO & COO.

### **C. Reporting and Incident Declaration Standards**

1. With the exception of the steps outlined below, it is imperative that any investigative or corrective action be taken only at the direction of the Chief Information Officer (CIO) to assure the integrity of the incident investigation and recovery process.

2. When faced with a potential situation, you should do the following:
  - a. If the incident involves a compromised computer system, do not alter the state of the computer system.
  - b. Report the security incident by contacting the CIO to report suspected or actual incidents.
  - c. Communications should remain internal, with supervisor(s) and CIO for initial assessment of any details or generalities surrounding the suspected or actual incident. The COO will coordinate all communications with law enforcement or the public.

#### **D. Incident Severity Classification**

1. The CIO will first attempt to determine whether the security incident justifies a formal incident response.
2. In cases where a security incident does not require an incident response, the issue will be forwarded to the appropriate area of IT to ensure that all technology support services required are executed.

## **VI. Anti-Malware Protection**

### General Use and Responsibilities:

All Louisiana Community and Technical College System (LCTCS) Board Office computer resources will be protected with one or more approved Anti-Malware software products.

### Policies and Procedures:

1. LCTCS CIO shall approve Anti-Malware software for use on all applicable IT resources. All Anti-Malware products shall be configured to receive automatic updates, perform periodic scans, and log events.
2. Users shall not change the configuration or disable the Anti-Malware software.
3. Anti-Malware software must be configured to automatically update signature data.
4. Systems running LCTCS Anti-Malware software shall alert IT Staff in real time of the detection of a virus.

## **VII. Definitions**

Cybercrime – Criminal activity or a crime that involves the Internet, a computer system, or computer technology.

Data breach – An incident in which sensitive, protected or confidential data has potentially been viewed, stolen or used by an individual unauthorized to do so. A data breach may involve personal health information (PHI), personally identifiable information (PII), trade secrets or intellectual property.

ISAP – Information Security Policy defines how the LCTCS Board Office IT resources shall be protected.

NPI – Non Public Information – LCTCS Board Office specific information such as financial documents, employee information, etc.

PCI – Payment Card Industry – Data Security Standard. Promotes Payment Card Industry standards for the safety of cardholder data across the globe.

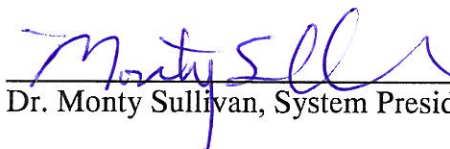
PII – Personally Identifiable Information – any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered PII.

User – Any person who makes any use of any LCTCS Board Office IT resource from any location (whether authorized or not).

AUTHORIZING SIGNATURES:

  
\_\_\_\_\_  
Joseph F. Marin, Chief Operations Officer

2/27/18  
\_\_\_\_\_  
Date

  
\_\_\_\_\_  
Dr. Monty Sullivan, System President

2/28/2018  
\_\_\_\_\_  
Date