

POLICIES AND PROCEDURES MANUAL

TITLE	Information Sensitivity Policy
LEGAL AUTHORITY	President and Cabinet
DATE APPROVED	November 7, 2005

1.0 Purpose

The Information 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 Lawson State Community 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 introduction. 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 Lawson State Community College Confidential information (e.g., Lawson State Community College Confidential information should not be left unattended in conference rooms).

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

Questions about the proper classification of a specific piece of information should be addressed to your manager. Questions about these guidelines should be addressed to MIS.

2.0 Scope

All Lawson State Community College information is categorized into two main classifications:

- Lawson State Community College Public
- Lawson State Community College Confidential

Lawson State Community College Public information is information that has been declared public knowledge by someone with the authority to do so, and can freely be given to anyone without any possible damage to Lawson State Community College.

Lawson State Community College Confidential contains all other information. It is a continuum, in that it is understood that some information is more sensitive than other information, and should be protected in a more secure manner. Included is information that should be protected very closely, such as student or employee social security

POLICIES AND PROCEDURES MANUAL

TITLE	Information Sensitivity Policy
LEGAL AUTHORITY	President and Cabinet
DATE APPROVED	November 7, 2005

numbers, development programs, and other information integral to the success of our institution. Also included in Lawson State Community College Confidential is information that is less critical, such as telephone directories, general college information, etc., which does not require as stringent a degree of protection.

Lawson State Community College personnel are encouraged to use common sense judgment in securing Lawson State Community 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 department head

3.0 Policy

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

3.1 Minimal Sensitivity: General institution information; some personnel and technical information

Marking guidelines for information in hardcopy or electronic form.

Note: any of these markings may be used with the additional annotation of "3rd Party Confidential".

Marking is at the discretion of the owner or custodian of the information. If marking is desired, the words "Lawson State Community College Confidential" may be written or designated in a conspicuous place on or in the information in question. Other labels that may be used include "Lawson State Community College Proprietary" or similar labels at the discretion of your department. Even if no marking is present, Lawson State Community College information is presumed to be "Lawson State Community College Confidential" unless expressly determined to be Lawson State Community College Public information by a Lawson State Community College employee with authority to do so.

Access: Lawson State Community College employees, contractors, people with a business need to know.

POLICIES AND PROCEDURES MANUAL

TITLE	Information Sensitivity Policy
LEGAL AUTHORITY	President and Cabinet
DATE APPROVED	November 7, 2005

Distribution within Lawson State Community College: Standard interoffice mail, approved electronic mail and electronic file transmission methods.

Distribution outside of Lawson State Community College internal mail: U.S. mail and other public or private carriers, approved electronic mail and electronic file transmission methods.

Electronic distribution: No restrictions except that it be sent to only approved recipients.

Storage: Keep from view of unauthorized people; erase whiteboards, do not leave in view on tabletop. Machines should be administered with security in mind. Protect from loss; electronic information should have individual access controls where possible and appropriate.

Disposal/Destruction: Deposit outdated paper information in specially marked disposal bins on Lawson State Community College premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.

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

3.2 More Sensitive: Business, financial, technical, and most personnel information

Marking guidelines for information in hardcopy or electronic form.

Note: any of these markings may be used with the additional annotation of "3rd Party Confidential". As the sensitivity level of the information increases, you may, in addition or instead of marking the information "Lawson State Community College Confidential" or "Lawson State Community College Proprietary", wish to label the information "Lawson State Community College Internal Use Only" or other similar labels at the discretion of your individual business unit or department to denote a more sensitive level of information. However, marking is discretionary at all times.

Access: Lawson State Community College employees and non-employees with signed non-disclosure agreements who have a business need to know.

Distribution within Lawson State Community College: Standard interoffice mail, approved electronic mail and electronic file transmission methods.

Distribution outside of Lawson State Community College internal mail: Sent via U.S. mail or approved private carriers.

POLICIES AND PROCEDURES MANUAL

TITLE	Information Sensitivity Policy
LEGAL AUTHORITY	President and Cabinet
DATE APPROVED	November 7, 2005

Electronic distribution: No restrictions to approved recipients within Lawson State Community College, but should be encrypted or sent via a private link to approved recipients outside of Lawson State Community College premises.

Storage: Individual access controls are highly recommended for electronic information.

Disposal/Destruction: In specially marked disposal bins on Lawson State Community College premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.

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

3.3 Most Sensitive: Student and employee personal information , operational, personnel, financial, source code, & technical information integral to the success of our Institution

Marking guidelines for information in hardcopy or electronic form.

Note: any of these markings may be used with the additional annotation of "3rd Party Confidential". To indicate that Lawson State Community College Confidential information is very sensitive, you may should label the information "Lawson State Community College Internal: Registered and Restricted", "Lawson State Community College Eyes Only", "Lawson State Community College Confidential" or similar labels at the discretion of your individual business unit or department. Once again, this type of Lawson State Community College Confidential information need not be marked, but users should be aware that this information is very sensitive and be protected as such.

Access: Only those individuals (Lawson State Community College employees and non-employees) designated with approved access and signed non-disclosure agreements.

Distribution within Lawson State Community College: Delivered direct - signature required, envelopes stamped confidential, or approved electronic file transmission methods.

Distribution outside of Lawson State Community College internal mail: Delivered direct; signature required; approved private carriers.

Electronic distribution: No restrictions to approved recipients within Lawson State Community College, but it is highly recommended that all information be strongly encrypted.

POLICIES AND PROCEDURES MANUAL

TITLE	Information Sensitivity Policy
LEGAL AUTHORITY	President and Cabinet
DATE APPROVED	November 7, 2005

Storage: Individual access controls are very highly recommended for electronic information. Physical security is generally used, and information should be stored in a physically secured computer.

Disposal/Destruction: Strongly Encouraged: In specially marked disposal bins on Lawson State Community College premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.

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

4.0 Enforcement

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

5.0 Definitions

Terms and Definitions

Appropriate measures

To minimize risk to Lawson State Community College from an outside business connection. Lawson State Community College computer use by competitors and unauthorized personnel must be restricted so that, in the event of an attempt to access Lawson State Community College information, the amount of information at risk is minimized.

Configuration of Lawson State Community College-to-other business connections
Connections shall be set up to allow other entities to see only what they need to see. This involves setting up both applications and network configurations to allow access to only what is necessary.

Delivered Direct; Signature Required

Do not leave in interoffice mail slot, call the mail room for special pick-up of mail.

Approved Electronic File Transmission Methods

Includes supported FTP clients and Web browsers.

Envelopes Stamped Confidential

You are not required to use a special envelope. Put your document(s) into an interoffice envelope, seal it, address it, and stamp it confidential.

POLICIES AND PROCEDURES MANUAL

TITLE	Information Sensitivity Policy
LEGAL AUTHORITY	President and Cabinet
DATE APPROVED	November 7, 2005

Approved Electronic Mail

Includes all mail systems supported by MIS.

Approved Encrypted email and files

Techniques include the use of DES and PGP. DES encryption is available via many different public domain packages on all platforms.

College Information System Resources

College Information System Resources include, but are not limited to, all computers, their data and programs, as well as all paper information and any information at the Internal Use Only level and above.

Expunge

To reliably erase or expunge data on a PC you must use a separate program to overwrite data. Otherwise, the PC's normal erasure routine keeps the data intact until overwritten.

Individual Access Controls

Individual Access Controls are methods of electronically protecting files from being accessed by people other than those specifically designated by the owner.

Insecure Internet Links

Insecure Internet Links are all network links that originate from a locale or travel over lines that are not totally under the control of Lawson State Community College.

Encryption

Secure Lawson State Community College Sensitive information in accordance with the *Acceptable Encryption Policy*. International issues regarding encryption are complex. Follow the institution guidelines on export controls on cryptography, and consult your department head for further guidance.

One Time Password Authentication

One Time Password Authentication on Internet connections is accomplished by using a one time password token to connect to Lawson State Community College's internal network over the Internet. Contact your support organization for more information on how to set this up.

POLICIES AND PROCEDURES MANUAL

TITLE	Information Sensitivity Policy
LEGAL AUTHORITY	President and Cabinet
DATE APPROVED	November 7, 2005

Physical Security

Physical security means either having actual possession of a computer at all times, or locking the computer in an unusable state to an object that is immovable. Methods of accomplishing this include having a special key to unlock the computer so it can be used, thereby ensuring that the computer cannot be simply rebooted to get around the protection. If it is a laptop or other portable computer, never leave it alone in a conference room, hotel room or on an airplane seat, etc. Make arrangements to lock the device in a hotel safe, or take it with you. In the office, always use a lockdown cable. When leaving the office for the day, secure the laptop and any other sensitive material in a locked drawer or cabinet.

Private Link

A Private Link is an electronic communications path that Lawson State Community College has control over its entire distance. For example, all Lawson State Community College networks are connected via a private link. A computer with modem connected via a standard land line (not cell phone) to another computer have established a private link. ISDN lines to employee's homes is a private link. Lawson State Community College also has established private links to other companies, so that all email correspondence can be sent in a more secure manner.

6.0 Revision History

PROCEDURES AND DEFINITIONS FOR INFORMATION SENSITIVITY POLICY

DEFINITIONS

Internet

A term to describe connecting multiple separate networks together.

Intranet

A computer network, especially one based on Internet technology, that an organization uses for its own internal, and usually private, purposes and that is closed to outsiders.

Extranet

A private network that uses Internet technology and the public telecommunication system to securely share part of a business's information or operations with suppliers, vendors, partners, customers, or other businesses.

FTP

File Transfer Protocol. A standard method for sending files from one computer to another on TCP/IP networks such as the Internet.

Virus

An executable or self-replicating program spread as a set of instructions that attaches itself and spreads to e-mail, programs, files, diskettes, or other storage media. The instructions can display a message, erase or alter files, stored data, or potentially render a workstation or network inoperable. Sometimes, instead of disruptive instructions, a virus can cause damage by replicating itself and depleting resources, such as disk space, memory or network connections.

Compromise

That the security of your computer or network is weakened.

Encryption

Encryption is taking your text, data or other communications and encoding it so that those who should not see or hear it will not be able to. An encrypted file will appear as gibberish unless you have the password or key necessary to decrypt the information.

Sniffing

Used to see what type of traffic is being passed on a network and to look for things like passwords, credit card numbers, and so forth. Sniffing is the term generally used for traffic monitoring within a network.

Pinged Floods

Ping Flood attacks attempt to saturate a network by sending a continuous series of ICMP echo requests (pings) over a high-bandwidth connection to a target host on a lower-bandwidth connection to cause it to send back an ICMP echo reply for each request. Ping Flood attacks can slow down a network or even disable network connectivity.

Packet Spoofing

A technique used by hackers to access computer systems by modifying packet headers to make them appear to have originated from a trusted port. 2. The practice of falsifying an e-mail header to make it appear as though it originated from a different address.

Denial of Service

An attack on a network designed to prevent the victim from using the network by flooding it with useless traffic.

Forged Routing Information

Routing information which is misleading or incorrect or which would tend to disguise the origin of the routed material. Usually refers to information that is not generated by any routing device (such as a mail server), but is inserted by a party using software which is designed to produce false routing information (headers in the case of E-mail).

Port Scanning

Running a program that attempts to learn about the weaknesses of a computer or network edge device by repeatedly probing it with requests for information.