

Information Sensitivity Standard

Revision Date:

1. Purpose: This policy is intended to help employees determine:

- What information can be disclosed to non-employees
- The relative sensitivity of information that should not be disclosed outside of El Paso Community College (EPCC) without proper authorization. Questions about the proper classification of a specific piece of information should be addressed to your manager. Questions about the guidelines should be addressed to management.

2. Scope: All EPCC information is categorized into two main classifications: public and confidential. Further designations are required when appropriate. 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 (e.g., telephone and video conferencing). All employees should familiarize themselves with the information labeling and handling guidelines that follow. The principal behind an information sensitivity policy is that only the intended audience or authorized individuals should see or have an opportunity to see information and only authorized individuals should be able to modify information. Exceptions to this are made only by those who have the authority to do so. 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 EPCC confidential information (e.g., EPCC confidential information should not be left unattended in conference rooms).

Public

EPCC public information is information that has been declared public knowledge by someone with the authority to do so and is consistent with Federal, State and EPCC regulations.

Sensitive

EPCC sensitive information 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, passwords, encryption keys, technical configuration files and other information integral to the protecting the people and infrastructure necessary to administer services to EPCC population.

Also included in EPCC sensitive information is information that is less critical, such as telephone directories, general organization information, etc., which does not require as stringent a degree of protection. A subset of EPCC sensitive information is “EPCC Third-Party confidential” information. This is confidential information belonging or pertaining to another organization that has been entrusted to EPCC by that organization

under non-disclosure agreements and other contracts. Examples of this type of information include everything from proprietary vendor tools to business partner connections. Information in this category ranges from extremely sensitive to information about the fact that the organization is collaborating with other service providers. EPCC personnel are encouraged to use common sense judgment in securing EPCC confidential information to the proper extent. If an employee is uncertain of the sensitivity of a particular piece of information, he or she should contact their manager.

3. Policy Description: The sensitivity guidelines below provide details on how to protect information at varying sensitivity levels. Use these guidelines as a reference only, as EPCC confidential information in each column may necessitate more or less stringent measures of protection, depending upon the circumstances and the nature of EPCC confidential information in question. A given sensitivity designation is assumed to stay in effect until explicitly changed by the information owner or someone in EPCC with the authority to do so.

Public Information

This is information available to anyone who asks based on legislative mandate, such as EPCC, State, and/or Federal regulations or declared to be public by someone within EPCC with the authority to do so. This information is to be provided via due process in order to ensure that the information is in fact public and that cost for providing the information is appropriately recovered. Public available information still requires access controls for authorized changes. Unless regulations demand otherwise, any information that is marked “Draft” or “Confidential” or “Sensitive” is not public by definition. If information is not marked or otherwise classified, EPCC information is presumed to be “sensitive” unless expressly determined to be EPCC public information by a EPCC employee with authority to do so. Unless you have the authority to interpret what is public information, verify requests through your manager.

Sensitive Information

Minimal Sensitivity

General organization information; some personnel and some general technical information.

- **Labeling**

Marking or labeling is at the discretion of the owner or custodian of the information. If marking is desired, the words “EPCC <Department Name> Sensitive” may be written or designated in a conspicuous place on or in the information in question. Other labels that may be used the discretion of your individual business unit or department.

- **Access:**

EPCC employees, contractors, people with a business need to know.

- **Distribution within EPCC:**

- o Standard interoffice mail

- o Approved electronic mail, and electronic file transmission methods.
- Distribution outside of EPCC internal mail:
 - o U.S. mail and other public or private carriers
 - o Approved electronic mail, and electronic file transmission methods.
- Electronic distribution:
 - o Must be sent to approved recipients.
- Storage:
 - o Keep from view of unauthorized people. E.g. erase whiteboards; do not leave in view on tabletop.
 - o Should not be stored or displayed on machines without physical and software access controls.
 - o Protect information from loss.

Any medium for backup/recovery should have the same or better access and security controls as the original data.

- o Electronic information should have individual access controls where possible and appropriate.
- o Information should not be stored in a given location any longer than the business function or regulation requires. E.g. Downloading files to telecommuting machines, laptops, PDA's etc.
- o Equipment that is no longer under the physical control of EPCC must have information expunged/cleared prior to transferring control to an outside agency. E.g. surplus, sending equipment out for repair, loaning equipment, etc.
- Disposal/Destruction:
 - o Shred outdated paper information
 - o Electronic data should be expunged/cleared
 - o 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.

More Sensitive

Financial, technical, and most personnel information.

- Labeling

Marking or labeling is at the discretion of the owner or custodian of the information. If marking is desired, the words "EPCC <Department Name> Confidential" may be written or designated in a conspicuous place on or in the information in question. Other labels that may be used the discretion of your individual business unit or department.

- Access

EPCC employees and non-employees with signed nondisclosure agreements who have a business need to know.

- Distribution within EPCC:

- o Standard interoffice mail
- o Approved electronic mail
- o Approved electronic file transmission methods.
- Distribution outside of EPCC internal mail:
 - o Sent via U.S. mail or approved private carriers.

- Electronic distribution:
 - Must be sent to only approved recipients.
 - Must be transmitted via a private link or encrypted securely when sent to approved recipients outside of EPCC premises.
- Storage:
 - Keep from view of unauthorized people
E.g. erase whiteboards; do not leave in view on tabletop.
 - Should not be stored or displayed on machines without physical and software access controls.
 - Protect information from loss.

Any medium for backup/recovery should have the same or better access and security controls as the original data.

- Electronic information should have individual access controls.
- Information should not be stored in a given location any longer than the business function or regulation requires.
- Information transferred to laptops, pda's and other portable media must be encrypted.
- Equipment that is no longer under the physical control of EPCC must have information expunged/cleared prior to transferring control to an outside agency.
E.g. surplus, sending equipment out for repair, loaning equipment, etc.
- Disposal/Destruction:
 - Shred outdated paper information
 - 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.

Most Sensitive

Operational, personnel, financial, source code, and technical information such as configurations, connectivity diagrams, patch procedures. Any information that could be used to impersonate a person or a process or lead to unauthorized access or modification of information.

- Labeling

Marking or labeling is at the discretion of the owner or custodian of the information. If marking is desired, the words "EPCC <Department Name> Classified" may be written or designated in a conspicuous place on or in the information in question. Other labels that may be used the discretion of your individual business unit or department.

- Access

Only those individuals (EPCC employees and non-employees) designated with approved access and signed nondisclosure agreements.

- Distribution within EPCC:

- Delivered direct — signature required, envelopes stamped confidential,
- Approved encrypted electronic file transmission methods.

- Distribution outside of EPCC internal mail:

- Delivered direct, signature required,

- o Approved private carriers.
- Electronic distribution:
 - o Must be sent to only approved recipients.
 - o Must be encrypted securely when sent to approved recipients outside of EPCC premises.
- Storage:
 - o Keep from view of unauthorized people
E.g. erase whiteboards; do not leave in view on tabletop.
 - o Should not be stored or displayed on machines without physical and software access controls.
 - o Protect information from loss.

Any medium for backup/recovery should have the same or better access and security controls as the original data.

- o Electronic information should have individual access controls.
- o Information should not be stored in a given location any longer than the business function or regulation requires.
- o Information transferred to laptops, PDA's and other portable media must be encrypted.
- o Equipment that is no longer under the physical control of EPCC must have information expunged/cleared prior to transferring control to an outside agency.
E.g. surplus, sending equipment out for repair, loaning equipment, etc.
- o Individual access controls are required for electronic information.
- o Individual access controls for physical security is required for all forms of storage.
- Disposal/Destruction:
 - o Shred outdated paper information
 - o Electronic data should be expunged/cleared
 - o 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. Enforcement: Violation of this standard may result in disciplinary action in accordance with El Paso Community College policy and procedures. Additionally, individuals are subject to loss of EPCC Information Resources access privileges, civil, and criminal prosecution. If you need clarification of this standard, call or e-mail Richard Buller, 831-6312, richardb@epcc.edu, from the Vice President for Information Technology/Chief Information Officer.

5. Definitions:

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

Approved electronic file transmission methods (Includes products supported by the IT support group.) [list organization supported transmission software here]
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.

Approved electronic mail: Includes all mail systems supported by the IT support group. These include, but are not necessarily limited to, [insert organization-supported mailers here]. If you have a business need to use other mailers, they must be approved by your management. (For example a personal Hot Mail account may not be an approved mailer.)

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. PGP use within EPCC is done via a license. Please contact the appropriate support organization if you require a license.

Configuration of EPCC-to-other business connections: Connections shall be set up to allow other businesses 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.

Encryption: Secure EPCC sensitive information in accordance with the Acceptable Encryption Policy. International issues regarding encryption are complex. Follow organization guidelines on export controls on cryptography, and consult your manager and/or organization legal services for further guidance.

Expunge: To reliably erase or expunge data, the data must be overwritten a number of times. If the operating system does not support this kind of erasure, a separate product may be required.

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. Authentication controls must be sufficient to validate the user according to the sensitivity of the information accessed. Careful planning and use of file and directory access permissions must be used to adequately authorize the access to the information.

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 EPCC.

Insecure Wireless link: A wireless link is an electronic communications path that transmits through the air using the radio spectrum. This connection can be between two computers or between computers and wireless access points. This link is considered insecure unless the SSID is not transmitted and encryption is configured and enforced.

One-time password authentication: One-time password authentication on Internet connections is accomplished by using a one-time password token to connect to EPCC's internal network over the Internet. Contact your support organization for more information on how to set this up.

Organization information system resources: Organization 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.

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 EPCC has control over its entire distance. For example, a computer with modem connected via a standard land line (not cell phone) to another computer have established a private link. ISDN lines to employees' homes are private links. EPCC also has established private some private links to other agencies.