

1.0 Confidentiality Policy

1.1. 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 Emphasys Software 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 employees can take to protect Emphasys Software Confidential information (e.g., Emphasys Software 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 a manager. Questions about these guidelines should be addressed to Human Resources.

1.2 Scope

All Emphasys Software information is categorized into two main classifications:

- Emphasys Software Public
- Emphasys Software Confidential
 - Client Confidential (subset of Emphasys Software Confidential)

Emphasys Software 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 Emphasys Software, Inc. Emphasys Software 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 trade secrets, development programs, potential acquisition targets, and other information integral to the success of our company. Also included in Emphasys Software Confidential is information that is less critical, such as telephone directories, general corporate information, personnel information, etc., which does not require as stringent a degree of protection.

A subset of Emphasys Software Confidential information is "Client Confidential" information. This is confidential information belonging or pertaining to another corporation which has been entrusted to Emphasys Software by that company under non-disclosure agreements and other contracts. Examples of this type of information include everything from joint development efforts to vendor lists, customer orders, and supplier information. Information in this category ranges from extremely sensitive to information about the fact that we've connected a supplier / vendor into Emphasys Software's network to support our operations.

Emphasys Software personnel are required to secure Emphasys Software Confidential (as well as subset Client 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 immediately.

1.3 Policy

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

Marking is at the discretion of the owner or custodian of the information. Even if no marking is present, Emphasys Software information is presumed to be "Emphasys Software Confidential" unless expressly determined to be Emphasys Software Public information by an Emphasys Software employee with authority to do so.

Any and all information deemed to be confidential under this policy must be properly disposed of or destroyed within 1 business day after business action is completed.

1.3.1 Minimal Sensitivity – “Emphasys Software Public”: General corporate information; some personnel and technical information

Access: Emphasys Software employees, contractors, people with a business need to know.

Distribution within Emphasys Software: Standard interoffice mail, approved electronic mail and electronic file transmission methods.

Distribution outside of Emphasys Software 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 Emphasys Software 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.

1.3.2 More Sensitive – “Emphasys Software Confidential”: Business, financial, technical, and most personnel information

Access: Emphasys Software employees and non-employees with signed non-disclosure agreements who have a business need to know.

Distribution within Emphasys Software: Standard interoffice mail, approved electronic mail and electronic file transmission methods.

Distribution outside of Emphasys Software internal mail: Sent via U.S. mail or approved private carriers.

1.3.3 Electronic distribution: No restrictions to approved recipients within Emphasys Software, but should be encrypted or sent via a private link to approved recipients outside of Emphasys Software premises.

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

Disposal/Destruction: In disposal bins on Emphasys Software 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.

1.3.4 Most Sensitive – Elements of “Emphasys Software Confidential” and all “Client Confidential”: Trade secrets & marketing, operational, personnel, financial, source code, & technical information integral to the success of our company and all Client Confidential Data

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 Emphasys Software Confidential information is very sensitive, consider labeling the information with "Emphasys Software Internal: Registered and Restricted", "Emphasys Software Eyes Only", "Emphasys Software Confidential" or similar labels as deemed by the affected individual business unit or department. Once again, this type of Emphasys Software Confidential information need not be marked, but users should be aware that this information is extremely sensitive and must be protected as such.

Access: Only those individuals (Emphasys Software employees and non-employees) designated with approved access and signed non-disclosure agreements.

Distribution within Emphasys Software: Delivered direct - signature required, envelopes stamped confidential, or approved electronic file transmission methods.

Distribution outside of Emphasys Software internal mail: Delivered direct; signature required; approved private carriers.

Electronic distribution: No restrictions to approved recipients within Emphasys Software, but all “Confidential” information must be strongly encrypted.

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 disposal bins on Emphasys Software 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.

1.4 Enforcement

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

1.5 Definitions

Terms	Definitions
Appropriate measures	To minimize risk to Emphasys Software from an outside business connection, Emphasys Software computer use by competitors and unauthorized personnel must be restricted so that, in the event of an attempt to access Emphasys Software corporate information, the amount of information at risk is minimized.
Configuration of Emphasys Software-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.
Approved Electronic File Transmission Methods	Includes supported FTP clients and Web browsers.
Envelopes Stamped Confidential	Special envelopes are not required. Put the document(s) into an interoffice envelope, seal it, address it, and stamp it confidential.
Approved Electronic Mail	Includes all mail systems supported by the Network Administrator. These include, but are not necessarily limited to Microsoft Exchange and Outlook. For business needs that require the use of other mailers contact the appropriate support organization.
Approved Encrypted email and files	Techniques include the use of PGP or GPG. DES encryption is available via many different public domain packages on all platforms. Please contact the Help Desk regarding approved encryption methods.
Company Information System Resources	Company 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, a separate program must 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. On PCs, this includes using passwords on screensavers.
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 Emphasys Software.
Encryption	Secure Emphasys Software Sensitive information in accordance with the Acceptable Encryption Policy. International issues regarding encryption are complex. Follow corporate guidelines on export controls on cryptography, and consult the Help Desk for further guidance.

Terms	Definitions
Physical Security	Physical security means either having actual possession of a computer at all times, or locking the computer in an unusable state. Methods of accomplishing this include having a domain username and password 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 keep it in person. When leaving the office for the day, secure the laptop and any other sensitive material in a locked drawer or cabinet. No information, equipment, or software belonging to Emphasys Software shall be removed from the premises without express authorization from executive management.
Private Link	A Private Link is an electronic communications path that Emphasys Software has control over its entire distance. For example, all Emphasys Software networks are connected via a private link. A computer with modem connected via a standard land line (not cell phone) to another computer has established a private link. Connections to employee's homes are private links.

Revision History

DATE	DESCRIPTION	REVISION NUMBER
10/1/18	Document creation	Rev. 0
11/9/18	Added timeframe to dispose or destroy confidential information under section 1.3 Policy	Rev. 1