

Information Sensitivity Policy and Procedure

Authorized By:	G. Franklin Lewis	Date Authorized:	3/16/2011
Effective Date:	4/1/2011	Last Amendment Date:	
Version Number:	1	Document Number:	PR-INT-CD-4009

Implementation & Review:	Bryan Chapman
Superseded Document:	
Related Documents:	

Any questions or concerns with this Policy and Procedure document should be referred to the first-line supervisor. If questions are not resolved, follow the organizational chart.

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 AboveTraining Inc. without proper authorization.

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

2.0 Scope

All AboveTraining Inc. information is categorized into two main classifications:

- AboveTraining Inc. Public
- AboveTraining Inc. Confidential

AboveTraining Inc. Public includes 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 AboveTraining Inc.

AboveTraining Inc. Confidential includes all other information. It is a continuum, in 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, learner information including driver license information, social security numbers, test outcomes, and other information integral to the success of our company, unless pertinent information is required by an AboveTraining Inc. customer. For example, a Health Department may require a driver license number be placed on a food handler certificate.

A subset of AboveTraining Inc. Confidential information is "AboveTraining Inc. Third Party Confidential" information. This is confidential information belonging or pertaining to another individual, customer, or corporation which has been entrusted to AboveTraining Inc. by that company under confidentiality policies or non-disclosure agreements and other contracts.

This type of information includes everything from joint development efforts to vendor lists, customer orders, and supplier information.

AboveTraining Inc. personnel are encouraged to use common sense judgment in securing AboveTraining Inc. 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 direct supervisor. At all times, employees of AboveTraining Inc. are governed by the company Confidentiality Agreement, which all employees are required to sign as a pre-requisite to starting employment.

3.0 Policy

The Sensitivity Guidelines below provide details on how to protect information at varying sensitivity levels. These guidelines are to be used as a reference only, as AboveTraining Inc. Confidential information may demand more or less stringent measures of protection depending upon the circumstances and the nature of the AboveTraining Inc. Confidential information in question.

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

Marking is at the discretion of the owner or creator of the information. If marking is desired, the words "AboveTraining Inc. Confidential" may be written or designated in a conspicuous place on or in the information in question. Even if no marking is present, AboveTraining Inc. information is presumed to be "AboveTraining Inc. Confidential" unless expressly determined to be AboveTraining Inc. Public information by an AboveTraining Inc. employee with authority to do so.

Access: AboveTraining Inc. employees, contractors, people with a business need to know.

Distribution within AboveTraining Inc.: Standard interoffice mail, approved electronic mail and electronic file transmission methods.

Distribution outside of AboveTraining Inc. 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 is 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 AboveTraining Inc. 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.

Marking is at the discretion of the owner or creator of the information. If marking is desired, the words "AboveTraining Inc. Confidential" may be written or designated in a conspicuous place on or in the information in question. Even if no marking is present, AboveTraining Inc. information is presumed to be "AboveTraining Inc. Confidential" unless expressly determined to be AboveTraining Inc. Public information by an AboveTraining Inc. employee with authority to do so.

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

Distribution within AboveTraining Inc.: Standard interoffice mail, approved electronic mail and electronic file transmission methods.

Distribution outside of AboveTraining Inc. internal mail: Sent via U.S. mail or approved private carriers.

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

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

Disposal/Destruction: In specially marked disposal bins on AboveTraining Inc. 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: Trade secrets & marketing, operational, personnel, financial, source code, & technical information integral to the success of our company

Any of these markings may be used with the additional annotation of "3rd Party Confidential". To indicate that AboveTraining Inc. Confidential information is very sensitive information should be labeled "AboveTraining Inc. Internal: Registered and Restricted", "AboveTraining Inc. Eyes Only", "AboveTraining Inc. Confidential" or similar labels at the discretion of the individual business unit or department. Once again, this type of AboveTraining Inc. Confidential information need not be marked, but users should be aware that this information is very sensitive and must be protected as such.

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

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

Distribution outside of AboveTraining Inc. internal mail: Delivered direct; signature required; approved private carriers.

Electronic distribution: No restriction to approved recipients within AboveTraining Inc., but it is highly recommended that all information 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 specially marked disposal bins on AboveTraining Inc. 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 AboveTraining Inc., computer use by non-employees or unauthorized personnel must be restricted so that the amount of information at risk is minimized.

Configuration of AboveTraining Inc.-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. This also includes providing access to only pertinent information, where information is to be shared, and only information that directly impacts those receiving information.

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.

Approved Electronic Mail

Includes all mail systems supported by the IT Support Team. These include, but are not necessarily limited to, AboveTraining Inc. approved electronic or hard copy mail campaigns. If you have a business need to use other mailers contact the appropriate support organization.

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 or Mac you must use a separate program to overwrite data, supplied as a part of Norton Utilities. Otherwise, the PC or Mac's normal erasure routine keeps the data intact until overwritten. The same thing happens on UNIX machines, but data is much more difficult to retrieve on UNIX systems.

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.

Unsecure Internet Links

Unsecure Internet Links are all network links that originate from a locale or travel over lines that are not totally under the control of AboveTraining Inc.

Encryption

Secure AboveTraining Inc. 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 your manager and/or corporate legal services 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 AboveTraining Inc.'s internal network over the Internet. Contact your support organization for more information on how to set this up.

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.

Private Link

A Private Link is an electronic communications path that AboveTraining Inc. has control over its entire distance.

6.0 Revision History