



Blue Ridge Community and Technical College Information Sensitivity Policy

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 Blue Ridge Community and Technical 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 BRCTC Confidential information (e.g., BRCTC 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 BRCTC.

2.0 Scope

All BRCTC information is categorized into two main classifications:

- BRCTC Public
- BRCTC Confidential

BRCTC 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 BRCTC Systems, Inc.

BRCTC 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 BRCTC Confidential is information that is less critical, such as telephone directories, general corporate information, personnel information, student identification and grades, etc., which does not require as stringent a degree of protection.

A subset of BRCTC Confidential information is "BRCTC Third Party Confidential" information. This is confidential information belonging or pertaining to another corporation which has been entrusted to BRCTC 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 BRCTC's network to support our operations.

BRCTC personnel are encouraged to use common sense judgment in securing BRCTC 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

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 BRCTC Confidential information in each column may necessitate more or less stringent measures of protection depending upon the circumstances and the nature of the BRCTC Confidential information in question.

3.1 **Minimal Sensitivity:** General corporate information; 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 "BRCTC Confidential" may be written or designated in a conspicuous place on or in the information in question. Other labels that may be used include "BRCTC Proprietary" or similar labels at the discretion of your individual business unit or department. Even if no marking is present, BRCTC information is presumed to be "BRCTC Confidential" unless expressly determined to be BRCTC Public information by a BRCTC employee with authority to do so.

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

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

Distribution outside of BRCTC 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 BRCTC 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 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 "BRCTC Confidential" or "BRCTC Proprietary", wish to label the information "BRCTC 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: BRCTC employees and non-employees with signed non-disclosure agreements who have a business need to know.

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

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

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

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

Disposal/Destruction: In specially marked disposal bins on BRCTC 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, student, financial, source code, & technical information integral to the success of our company

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 BRCTC Confidential information is very sensitive, you may should label the information "BRCTC Internal: Registered and Restricted", "BRCTC Eyes Only",

"BRCTC Confidential" or similar labels at the discretion of your individual business unit or department. Once again, this type of BRCTC 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 (BRCTC employees and non-employees) designated with approved access and signed non-disclosure agreements.

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

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

Electronic distribution: No restrictions to approved recipients within BRCTC, 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 BRCTC 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 BRCTC from an outside business connection. BRCTC computer use by competitors and unauthorized personnel must be restricted so that, in the event of an attempt to access BRCTC corporate information, the amount of information at risk is minimized.

Configuration of BRCTC-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.

BRCTC

Blue Ridge Community and Technical College

Delivered Direct; Signature Required

Do not leave in interoffice mail slot, hand deliver.

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. 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 approved by IT Services to overwrite data. Otherwise, the PC or Mac'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 Mac's and PC's, 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 BRCTC.

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.

6.0 Revision History

I, _____, acknowledge I have received, read, and understand the Blue Ridge Community and Technical College Information Sensitivity Policy.

Signature

Date

Print Name

I, _____, acknowledge I have received, read, and understand the Blue Ridge Community and Technical College Information Sensitivity Policy.

Signature

Date

Print Name