CARBON CAREER & TECHNICAL INSTITUTE

SECTION: OPERATIONS

TITLE: DATA BREACH POLICY

ADOPTED: June 18, 2015

REVISED:

	816. DATA BREACH POLICY
1. Policy	With the increased reliance upon electronic data, and the maintenance of personal information of students and employees in electronic format, the Joint Operating Committee is concerned about the risk of a breach in the Carbon Career & Technical Institute ("School") electronic system security and the possible disclosure of personal information. It is the policy of the School that employees comply with the Pennsylvania mandated identity theft prevention laws, including the Breach of Personal Information Notification Act and the Confidentiality of Social Security Number law, the federal Health Information Technology for Economic and Clinical Health Act ("HITECH Act"), and accompanying Health and Human Services ("HHS") regulations, and the School's procedures, including the Data Breach Prevention Plan, the Data Breach Incidence Response Plan, the Student Records Policy, and the Student Records Plan. Employees are required to protect the sensitive personally identifiable information about students, employees and others from inadvertent, negligent and willful disclosure or breach of such information, data or records. Violation of this Policy may result in corrective action up to and including termination.
2. Authority	The Board directs that School administrators shall provide appropriate notification of any security breach to any resident whose unencrypted, unredacted, and unsecure personal information was or is reasonably believed to have been accessed or acquired by unauthorized persons.
73 P.S. §2302	**A. <u>Pennsylvania Data Breach Notification for Personal Information</u>** **Breach of the system's security** – unauthorized access and acquisition of computerized data that materially compromises the security or confidentiality of personal information maintained by the School as part of the database of personal information regarding multiple individuals and that causes or the School reasonably believes has caused or will cause loss or injury to any Pennsylvania resident. Good faith acquisition of personal information by an employee or agent of the School for the purpose of the School is not a breach of the security of the system if the personal information is not used for a purpose other than the lawful purpose of the School and is not subject to further unauthorized disclosure.

73 P.S. § 2302	**Personal information** – includes an individual's first name or first initial and last name in combination with and linked to any one or more of the following, when not encrypted or redacted: 1. Social Security number. 2. Driver's license number or a state identification card number issued in lieu of a driver's license. 3. Financial account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to an individual's financial account.
73 P.S. § 2302 Policy 801	Personal information does not include publicly available information that is lawfully made available to the general public from federal, state or local government records.
73 P.S. § 2302	**Records –** pursuant to the Breach of Personal Information Notification Act, records mean any material, regardless of its physical form, on which information is recorded or preserved by any means, including written or spoken words, graphically depicted, printed or electromagnetically transmitted. The term does not include publicly available directories containing information an individual has voluntarily consented to have publicly disseminated or listed, such as name, address or telephone number. All employees must protect and secure all electronic resources and information, data and records of the School from theft, and inadvertent disclosure when they are under the supervision and control of the School, and when they not under the supervision or control of the School, for example, but not limited to, working at home, on vacation, or elsewhere. If any employee becomes aware of the release of School information, data or records the release must be reported to the Administrative Director immediately.
73 P.S. § 2302	The Administrative Director or designee shall provide notice of any system security breach of computerized records, following discovery of the breach of the security of the system, to any Pennsylvania resident whose unencrypted and unredacted personal information was, or is reasonably believed to have been accessed and acquired by an authorized person, without unreasonable delay.
73 P.S. § 2303	The School will also provide notice of the breach (a) if the encrypted information is accessed and acquired in an unencrypted form, (b) if the security breach is linked to a breach of the encryption, or (c) if the security breach involves a person with access to the encryption key. The School must report the breach of the security and any information pertaining to the breach to the local, state, or federal law enforcement agency for investigation or

	handling in advance of the disclosure to any resident, or others. The School may be required to delay notification if a law enforcement agency, determines and provides in writing that the notification will impede a criminal or civil investigation. The School must take necessary measures to determine the scope of the breach and to restore the reasonable integrity of the data system. The School administration must then determine whether a data breach notification will be issued. Notifications shall be provided by at least one (1) of the following methods: 1. Written notice, to last known home address for the individual. 2. Telephone notice, if the individual can be reasonably expected to receive the notice and the notice is given in a clear and conspicuous manner, describes the incident in general terms, and verifies personal information but does not require the individual to provide personal information, and the individual is provided a telephone number to call or Internet web site to visit for further information or assistance. 3. E-mail notice, if a prior business relationship exists and the School has a valid e-mail address for the individual. 4. Substitute notice, if the School determines that the cost of providing the notice exceeds $100,000, the affected individuals exceeds 175,000 persons, or the School does not have sufficient contact information. Substitute notice shall consist of an e-mail notice if the School has an e-mail address for the persons, conspicuous posting of the notice on the School's web site, and notification to major Statewide media. If the School provides notification to more than 1,000 persons at one (1) time, the School shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis as defined in the Fair Credit Reporting Act of the timing, distribution and number of notices.
HITECH Act, 45 C.F.R. Parts 160 & 164	**B. <u>Personal Health Information Data Breach</u>** 1. The School must protect the privacy and security of "protected health information" ("PHI"). Unless the PHI is encrypted or destroyed pursuant to the U.S. Department of Health and Human services ("HHS") standards and considered secure health information the School must comply with the HHS breach notification rules. 2. The HHS Breach Notification Rule requires covered entities to notify each individual whose unsecured PHI has been, or is reasonably believed to have

	been accessed, acquired, used, or disclosed following a breach of that unsecured PHI. The Rule also requires a business associate to notify the School of a breach of unsecured PHI. HHS sets forth the following three step process for covered entities to follow in determining whether a breach has occurred for which notification must be given: a. Determine whether there has been an impermissible use or disclosure of PHI under the HIPAA Privacy Rule; b. Determine, and document, whether the impermissible use or disclosure compromises the privacy or security of the PHI by having created a significant risk of financial, reputational, or other harm to the individual; and c. Determine whether the incident is excluded from the definition of "breach" because it is: • An unintentional use of PHI by a workforce member acting in good faith and within the scope of his or her authority, and the PHI is not further used or disclosed improperly; • An inadvertent disclosure of PHI by an authorized person to another authorized person, and the PHI is not further used or disclosed improperly; or • A disclosure of PHI to an unauthorized person where there is a good faith belief that the unauthorized person would not reasonably have been able to retain the PHI. 3. The Rule requires notice of a breach of unsecured PHI to be provided as follows: **a. Timeliness of Notification to the Individual** – Notification must be made to individuals "without unreasonable delay" but no later than 60 calendar days after discovery of the breach. Breaches must be treated as discovered on the first day that the breach is known to the School (i.e., known to any member of the School's workforce or agent of the School), or when, by exercising reasonable diligence, the breach would have been known to the School. **b. Content of Notification** – Notification sent to individuals must be "in plain language" and include the following: • A brief description of what happened, including the date of the breach and the date of discovery of the breach, if known; • A description of the types of unsecured PHI that were involved in
45 C.F.R. Part 164.404	

	the breach; • Steps individuals should take to protect themselves from potential harm resulting from the breach; • A brief description of the steps the School is taking to investigate the breach, mitigate harm, and protect against future breaches; and • Contact procedures for individuals to ask questions or obtain additional information, including a toll-free number, email address, website, or postal address.
45 C.F.R. Part 1164.404	**c. Methods of Notification to Individuals** – Notification to individuals must be sent to the individual's last known address via first-class mail, or email if the individual has agreed to email and has not withdrawn such agreement. If the contact information for less than 10 individuals is outdated or insufficient, substitute notice may be provided by an alternative written notice, telephone, or other means. However, if the contact information for 10 or more individuals is found to be outdated or insufficient, the School must provide substitute notice in one of the following forms: • Conspicuous posting on the home page of the School's website for a period of not less than 90 days; or • In major print or broadcast media, including in the areas where the affected individuals likely reside. In addition, the substitute notice on the website or in print or broadcast media must include a toll-free telephone number that will remain active for 90 days where individuals can learn whether their unsecured PHI was included in the breach.
45 C.F.R. Part 164.406	**d. Notification to Media** – If the breach affects more than 500 or more residents of a particular state or jurisdiction, the School also must notify "prominent media outlets" of the state or jurisdiction of the breach without unreasonable delay, but no later than 60 calendar after discovery of the breach.
45 C.F.R. Part 164.408	**e. Notification to HHS** – If the breach affects more than 500 individuals, notice must be made to HHS contemporaneously with the notification to the affected individuals. If fewer than 500 individuals are affected, the covered entity must maintain a log of any such breaches, and submit the log annually to HHS no later than 60 days following the end of the calendar year.

45 C.F.R. Part 164.410

f. Notification by Business Associates – Business associates must provide breach notification to Schools "without unreasonable delay" and in no case later than 60 calendar days after discovery of the breach. The Business Associate must, to the extent possible, provide the School with the identification of each individual whose PHI was breached, and any other information available that the School will need to notify the affected individuals.

HITECH Act, 45 C.F.R. Parts 160 & 164

C. <u>Destruction of School Records</u>

All records of the School must be destroyed pursuant to the School Document Retention and Destruction Policy, schedule and procedures. Destruction means shredding, erasing, or modifying the information in and of the records to make the records unuseable, unreadable, indecipherable or non- reconstructionable through generally available means. Protected Health Information must be destroyed pursuant to the National Institute of Standards and Technology ("NIST") security standards.

74 P.S. § 201

D. <u>Social Security Number Requirement</u>

Unless otherwise permitted by law, School employees must protect the privacy of Social Security numbers.

<u>The School may **not** do any of the following</u>:

1. Publicly post or publicly display in any manner an individual's Social Security number. "Publicly post" or "publicly display" means to intentionally communicate or otherwise make available the Social Security number to the general public.

2. Print an individual's Social Security number on any card required for the individual to access products or services provided by School.

3. Require an individual to transmit his or her Social Security number over the Internet unless the connection is secure or the Social Security number is encrypted.

4. Require an individual to use his or her Social Security number to access an Internet website unless a password or unique personal identification number or other authentication device is also required to access the website.
5. Print an individual's Social Security number on any materials that are mailed to the individual unless federal or state law requires the Social Security number to be on the document to be mailed. However, Social Security numbers may be included in applications and forms sent by mail, including documents sent as part of an application or enrollment process or to establish, amend or terminate an account, contract or policy or to confirm the accuracy of the Social Security number. A Social Security number that

	is permitted to be mailed under this section may not be printed, in whole or in part, on a postcard or other mailer not requiring an envelope, or visible on the envelope or without the envelope having been opened. 6. Disclose in any manner the Social Security number of an individual who applies for a recreational license (i.e., a fish or game license). The School may collect, use, or release a Social Security number as required by federal or state law or may use the Social Security number for internal verification, administrative purposes or for law enforcement investigations. This requirement does not apply to a document that is required by law to be open to the public, and originates with, or is filed, recorded or maintained by any court component or part of the unified judicial system. References: Breach of Personal Information Notification Act – 73 P.S. § 2301 et seq. Fair Credit Reporting Act – 15 U.S.C. § 1681a Family Educational Rights and Privacy Act – 20 U.S.C. § 1232g, 34 C.F.R. Part 99 HITECH Act – 45 C.F.R. Part 160 Pennsylvania Student Records Law – 22 Pa. Code § 12.31 - § 12.32 Social Security Number Law – 74 P.S. § 201 Public Records Board Policy – 801