BERKSHIRE COMMUNITY COLLEGE

Version: 1.1
Issued: 6/05/2018

Information Security Plan - BCC 38

1. Objective

Berkshire Community College's ("the College" or "BCC"), objective in the development and implementation of this Information Security Plan ("ISP" or "Plan"), is to create effective administrative, technical and physical safeguards for the protection of Confidential Information including the personal information of applicants, students, employees, alumni, and friends of the College, any of the College's sensitive business information that must be kept confidential, and to comply with our obligations under Massachusetts regulations.[1-5] This Plan sets forth our procedures for evaluating our electronic and physical methods of accessing, collecting, storing, using, transmitting, protecting, and disposing of the confidential information of anyone who conducts business with the College and are further detailed in BCC's Written Information Security Program (WISP).

For purposes of this Plan, "personal information" is defined as an individual's first name and last name, or first initial and last name, in combination with any one or more of the following data elements that relate to such resident: (a) Social Security Number; (b) driver's license number or state-issued identification card number; or (c) financial account number or credit or debit card number, with or without any required security code, access code, personal identification number, or password that would permit access to a resident's financial account where BCC is the custodian of that data; provided however, that personal information shall not include information that is lawfully obtained from publically available information, or from federal, state or local government records lawfully made available to the general public.[2]

2. Purpose

The purpose of this Plan is to:

1. Ensure the security and confidentiality of sensitive personal and business information;
2. Protect against any potential threats or hazards to the security or integrity of such information; and
3. Protect against unauthorized access to, or use of, such information in a manner that creates a substantial risk of identity theft or fraud.

3. Scope

In formulating and implementing the ISP, the College will (1) identify reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal or business information; (2) assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of the confidential information; (3) evaluate the sufficiency of existing policies, practices, procedures, information systems, and other safeguards in place to control risks; (4) design and implement a plan that puts safeguards in place to minimize those risks, consistent with the requirements of 201 CMR 17.00[1]; and (5) regularly monitor the Plan.

4. Data Security

BCC has designated Arlen Rauschkolb, Director of Information Technology, as its Chief Information Security Officer (CISO) to implement, supervise and maintain the Plan. In coordination with BCC administrators and IT system managers, the CISO will be responsible for:

1. Initial implementation of the ISP;
2. Oversight of ongoing employee training, provided through the Department of Human Resources, for all owners, managers, employees and independent contractors that have access to confidential information;
3. Monitoring the Plan's safeguards;
4. Assessing Third Party Service Providers that have access to and/or host/transmit/backup/maintain confidential information and requiring those service providers by College Policy and contract to implement and maintain such appropriate security measures for confidential information;
5. Reviewing the scope of the security measures whenever there is a material change in our business practices that may impact the security or integrity of records containing confidential information;
6. Reviewing legislation and laws and updating policies and procedures as required.

5. Internal Risks

To combat internal risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal or business information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, the following measures are mandatory and effective as of 6/29/2018:

<u>Administrative measures:</u>

- The amount of personal information collected must be limited to the amount reasonable necessary to accomplish the College's legitimate business purposes. This risk will be addressed through security audits in various areas.
- All data security measures shall be reviewed whenever there is a material change in our business practice that may reasonably impact the security or integrity of records containing confidential information. The CISO shall be responsible for this review and shall fully apprise management of the results of that review and any recommendations for improved security arising from that review.
- Through the Data Confidentiality clause of the College's Acceptable Use Policy, staff members and Third Party Service Providers are prohibited from any unauthorized use of personal information and "may be subject to civil and/or criminal liability" for any violation.
- Whenever there is an incident that requires notification under M.G.L. c 93H[3], there shall be an immediate mandatory post-incident review of events and actions taken, if any, with

a view to determining if changes in our security practices are required to improve the security of the confidential information for which we are responsible.

Physical measures:

- Access to records containing personal or business information shall be limited to those persons who are reasonably required to know such information in order to accomplish our legitimate business purpose. This risk is being addressed through redaction of sensitive information, storing paper records in locked facilities and implementing data security controls for electronic records.
- At the end of the work day, all files and other records containing personal information must be stored in locked in rooms, offices, or cabinets.
- Paper records containing personal information shall be disposed of in a manner that complies with M.G. L. c 93I[4].

Technical measures:

- When employees who have access to personal or business information are terminated, BCC terminates their access to network resources and physical devices that contain "personal information". This includes termination or surrender of network accounts, database accounts, keys, badges, phones, and laptops or desktops.
- Employees are required to change their passwords, at a minimum, semi-annually for systems that contain confidential information.
- Access to personal information shall be restricted to active users and active user accounts only.
- Where technically possible, all BCC maintained systems that store confidential information will employ automatic locking features which lock access after multiple unsuccessful login attempts.
- Electronic records (including records stored on hard drives and other electronic media) containing personal information shall be disposed of in a manner that complies with M.G. L. c 93I. This requires that information be destroyed or erased so that personal information cannot practicably be read or reconstructed.

6. External Risks

To combat external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing confidential information and evaluating or improving where necessary the effectiveness of the current safeguards for limiting such risks, the following measures are mandatory and effective as of 6/29/2018:

- There is a reasonably up-to-date firewall protection and operating system security patches designed to maintain the integrity of the personal information installed on systems with confidential information.
- There are reasonably up-to-date versions of system security agent software that includes malware protection and reasonably up-to-date patches and virus definitions installed on systems processing confidential information.

Pertinent Massachusetts Regulations:

1 201 CMR 17.00 - Standards for the Protection of Personal Information of Residents of The Commonwealth
2 201 CMR 17.02 - Definitions
3 M. G. L. c 93H - Security Breaches
4 M. G. L. c 93I - Dispositions and Destruction of Records
5 WISP - A Small Business Guide: Formulating A Comprehensive Written Information Security Program