Greenfield Community College

Written Information Security Plan
Version 1.1
Document History

<table>
<thead>
<tr>
<th>Date</th>
<th>Version</th>
<th>Change</th>
<th>Section/Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>05/2019</td>
<td>Draft</td>
<td>Creation</td>
<td>All</td>
</tr>
<tr>
<td>9/2019</td>
<td>Draft</td>
<td>Updates and edits</td>
<td>All</td>
</tr>
<tr>
<td>2/2020</td>
<td>Version</td>
<td>Updates</td>
<td>Various</td>
</tr>
</tbody>
</table>

Policy Information

<table>
<thead>
<tr>
<th>Policy Title</th>
<th>Information Security Program</th>
</tr>
</thead>
<tbody>
<tr>
<td>Functional Owner/Title</td>
<td>Laura Garcia</td>
</tr>
<tr>
<td>Policy Author/Title</td>
<td>Laura Garcia, CIO</td>
</tr>
<tr>
<td>Version</td>
<td>1.1</td>
</tr>
<tr>
<td>Date Approved</td>
<td></td>
</tr>
<tr>
<td>Effective Date</td>
<td>February 2020</td>
</tr>
<tr>
<td>Date of Last Review</td>
<td>February 2020</td>
</tr>
<tr>
<td>Date of Last Revision</td>
<td>February 2020</td>
</tr>
<tr>
<td>Replaces</td>
<td>1.0</td>
</tr>
<tr>
<td>Compliance References</td>
<td>MA 201 CMR 17.00 Standards for the Protection of Personal Information</td>
</tr>
</tbody>
</table>
Introduction

The protection of sensitive information is a critical component to the successful operation of any organization. Therefore, pursuant to the State of Massachusetts (MA) 201 CMR 17.00: “Standards for the Protection of Personal Information of Residents of the Commonwealth” and Massachusetts General Laws Chapter 93H, Greenfield Community College (GCC), has defined the steps necessary to evaluate the security risks and safeguards in relation to the size, scope and nature of the business processes and the potential risks of authorized access or use of sensitive and personally identifiable information (PII).

For purposes of this Written Information Security Program (WISP), “personally identifiable information” is defined in the MA 201 CMR 17.00 regulation:

- A Massachusetts resident’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:
  - Social Security number;
  - driver’s license number or state-issued identification card number; or
  - 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; provided, however, that “personal information” shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

Additional factors that require the protection of personal data include:

- Family Educational Rights and Privacy Act (FERPA) that governs the access to educational information and records by public entities.
- Various U.S. states with legislation on the protection of personal and/or consumer information.

Objective

This document is meant to define the high-level security requirements for Greenfield Community College to operate securely. It is assumed the additional detailed requirements will be captured in separate security procedure documents.

This WISP describes the methods to be used with administrative, technical and physical safeguards for the protection of PII in order to comply with requirements specified in the MA 201 CMR 17.00. This includes procedures to evaluate electronic and physical methods of accessing, collecting, storing, using, transmitting and protecting PII or sensitive data.

Greenfield Community College will strive to ensure all critical assets, such as information and technology, are identified and safeguarded appropriately. Furthermore, the purpose of this WISP is to:

- Ensure the security of sensitive data and PII;
- Protect against any anticipated threats or hazards to the security, confidentiality and integrity of such information;
- Protect against unauthorized access to, or use of such information, in a manner that creates substantial security or privacy risk.
Scope

The scope of this policy includes all departments within GCC that are connected to the computer network and/or that process, store, or transmit sensitive information (i.e. PII) either electronic or hardcopy form.

All members of the workforce (i.e. employees, whether full or part time, including contract, temporary workers, hired consultants, interns, student employees or third-party service providers) must adhere to this policy.

In the development and implementation of the WISP, GCC addressed and incorporated the following procedures:

- Identify any foreseeable internal and external risks to the security, confidentiality, and integrity of sensitive customer or PII data in the electronic, physical, or intellectual form;
- Assess the likelihood and potential damage of these threats, given the sensitivity of the information;
- Evaluate the sufficiency of existing policies, procedures, information systems and other safeguards in place to control risks;
- Design and implement safeguards to minimize those risks, consistent with industry accepted practices, standards, and the requirements of MA 201 CMR 17:00;
- Regularly monitor the effectiveness of those safeguards.

Data Security Coordinator

Responsible for the oversight and implementation for the WISP is:

Laura Garcia (413-775-1318 or GarciaL@gcc.mass.edu)

This designated employee (Data Security Administrator) will:

- Oversee and implement this WISP;
- Ensure that the Greenfield Community College workforce understands how to identify sensitive data and apply safeguards for protecting sensitive data and/or PII;
- Regularly test security safeguards;
- Ensure that the Greenfield Community College’s third-party contracts include requirements to implement and maintain appropriate security measures to safeguard sensitive customer data and/or PII;
- Evaluate the ability of each of the Greenfield Community College’s third-party service providers and contractors to implement and maintain appropriate security safeguards for sensitive customer data and PII which they have been permitted access;
- Ensure that any certifications and credentials are current and in good standing;
- Review and update this document annually, or whenever there is a material change in the business practices that may implicate the security, integrity or confidentiality of sensitive information or PII.
- Chair the Information Security Committee and facilitate meetings.
Information Security Committee

This policy shall be maintained and kept up-to-date by the GCC Information Security Committee, and its members:

- Data Security Coordinator and Chief Information Officer – Laura Garcia, Chair
- Finance’s Representative – Karen Phillips, CFO
- Administration’s Representative – Mary Ellen Fydenkevez, CLO
- GCC Human Resources Representative – Joan Murphy, Executive Director of HR

The Information Security Committee provides guidance and oversight on the implementation of this WISP and ensures that compensating controls are in place to reduce the risk associated with noncompliance.

This policy shall be reviewed annually (at a minimum) and updated, based on major changes in the environment or related to the processing of sensitive information.

Information Security Risks and Safeguards

To mitigate potential risks in the security, integrity and/or confidentiality of sensitive information or PII in any form (electronic, physical or intellectual) and in direct support of compliance with MA 201 CMR 17:00, the following tasks need to be performed:

Administrative Safeguards

1. A copy of the WISP must be distributed to each member of the workforce who shall, upon receipt, acknowledge in writing that he/she has received a copy.

2. Employment contracts must require complete compliance with the WISP and prohibit any non-conforming use of sensitive information and PII during or after employment. Anyone who violates the WISP is subject to mandatory disciplinary actions. The nature of the disciplinary measures will depend on the nature of the violation and the type of information affected by the violation.

3. The Data Security Coordinator and the department heads will maintain a list of business processes, applications and computer systems that use, store or process sensitive information and PII in order to establish and support safeguards for appropriate use.

4. The quantity of student-, staff- and faculty-sensitive information and PII collected should be limited to that which is reasonably necessary to accomplish legitimate business purposes, or essential to comply with other state and federal regulations.

5. Access to any sensitive data and PII shall be limited to persons required to know such information in order to accomplish the legitimate business purpose, or to enable the Greenfield Community College to comply with other state or federal regulations.

6. Sensitive information and PII shall not be removed from the college premises in electronic or written form absent legitimate business need and use of reasonable security measures, as described in this policy.
7. All security measures and safeguards shall be reviewed at least annually, or whenever there is a material change in the business practices that may implicate the security, integrity, or confidentiality of sensitive information or PII.

8. Terminated employees and contractors must return all materials containing sensitive data and PII including physical copies and all information on laptops or portable devices. If sensitive data and/or PII resides on personally owned equipment, the individual must destroy the data and sign a statement attesting to the destruction of the data/PII in a manner complying with M.G.L. c. 93I (Standards for disposal of records containing personal information; disposal by third party; enforcement).

9. All students and members of the Greenfield Community College workforce must report any suspicious activity or unauthorized use of sensitive information and PII to the Data Security Coordinator as soon as it is discovered.

10. Students and any personnel on site after normal business hours who are not authorized to have access to personal information cannot have access to areas where files containing personal information are stored.

11. Whenever there is an incident requiring notification under M.G.L. c. 93H, §3 (Duty to report known security breach or unauthorized use of personal information), there shall be an immediate mandatory post-incident review. Events and actions taken are to be examined to determine whether any security practice changes are required to secure any personal information.

Technical Safeguards

1. Electronic access to sensitive information and PII must be blocked after 5 unsuccessful attempts to gain access.

2. A terminated employee or contractor’s physical and electronic access to sensitive information and/or PII must be immediately blocked.

3. Current employee and contractor user IDs and passwords must be changed periodically (minimum of every 180 days).

4. Access to sensitive information and PII shall be restricted to active users and active user accounts only.

5. Any device (laptop, desktop, tablet, smart phone) in the possession of any employee or contractor must be restricted from accessing sensitive information or PII when not in use.

6. Access to electronically stored sensitive information and PII shall be electronically limited to those employees with a unique login ID, and a re-log-in shall be required when a computer has been inactive for more than 30 minutes.

7. The IT environment(s) shall include reasonably up-to-date firewall protection, anti-virus, anti-malware, and current operating systems with appropriate security patches on all servers and endpoint systems processing sensitive information and PII. This includes systems owned and used by students, employees and contractors.
8. The IT environment(s) must be reasonably up-to-date on versions of system security agent software which must include malware protection and reasonably up-to-date patches and virus definitions installed on all systems processing sensitive information and PII. This includes systems owned and used by students, employees and contractors.

9. All sensitive information and PII stored on laptops or other portable devices must be encrypted. To the extent technically feasible, all sensitive information and PII transmitted across public networks or wirelessly, must also be encrypted. PII encryption means the transformation of data into a form in which meaning cannot be assigned without the use of a confidential process or key, unless further defined by regulation by the Massachusetts Office of Consumer Affairs and Business Regulations.

10. All computer systems within the Greenfield Community College IT environment(s) must be monitored for unauthorized use of, or access to, sensitive information and PII.

11. The Greenfield Community College’s IT environment(s) must use secure user authentication protocols in place, including:
   a. Protocols for control of user IDs and other identifiers;
   b. A reasonably secure method of assigning and selecting passwords, or the use of unique identifier technologies, such as biometrics or token devices;
   c. Control of data security passwords to ensure such passwords are kept in a secure/encrypted location.

Physical Safeguards
1. Employees and contractors shall practice the Clean Desk Policy. At the end of each workday or when an employee is away from his/her desk for a period of time, all files and other records containing sensitive information or PII must be secured in a manner consistent with protecting the security, integrity and confidentiality of the data.

2. A terminated employee or contractor shall be required to surrender all keys, IDs or access codes or badges, business cards, and the like, that permit access to the Greenfield Community College Offices/premises or information. Moreover, the individual’s remote electronic access to the Greenfield Community College’s electronic systems must be disabled. His or her voice mail access, email access, Internet access, and passwords must be invalidated. The Data Security Administrator shall maintain a highly secured master list of all lock combinations, passwords, and keys, as appropriate.

3. Each department shall develop rules for each business function that uses or processes stored sensitive information or PII. Reasonable restrictions regarding physical access to sensitive information and PII must be in place. Written procedures must define how physical access to data in that functional area is to be restricted. And each function must store sensitive data in locked facilities, secure storage areas or locked containers.

4. Visitor access must be restricted for office areas that use, process or store sensitive information or PII. Visitors shall not be permitted to be unescorted in any area within the premises that contains sensitive customer data and PII.

5. Paper or electronic records, including records stored on hard drives or other electronic media containing personal information shall be disposed of, in compliance with M.G.L. c. 93I (Standards for disposal of records containing personal information; disposal by third party; enforcement).
Daily Operational Safeguards
This section of the WISP outlines the safeguards used to minimize the security risks to any physically or electronically sensitive data or PII. Information is to be secured and processes designed to minimize access and security risks to personal information used, processed or stored within our environment.

Any modifications to the daily operational protocol shall be published in an updated version of the WISP. At the time of publication, a copy of the WISP shall be distributed to all current employees and to new hires on their date of employment.

1. We will only collect personal information from students and employees that is necessary to accomplish our legitimate business transactions or to comply with any and all federal and state and local laws.

2. The Data Security Coordinator, his/her designee and/or department manager, shall perform an assessment of all relevant records to determine which records contain PII. These files must be assigned to the appropriate secured storage location, and all necessary PII redacted or eliminated in a manner consistent with the WISP.

3. Any PII stored shall be disposed of when no longer needed for business purposes or required to be stored by law. Disposal methods must comply with the WISP.

4. Any paper files containing PII shall be stored in a locked filing cabinet. Only department heads and the Data Security Coordinator will be assigned keys to the filing cabinets. Only those individuals with a “need to know” are allowed access to the paper files. Individual files may be assigned to employees on a “need to know” basis by the department supervisor.

5. All employees are prohibited from keeping unsecured paper files containing PII in their work area when they are not present (e.g., when attending lengthy meetings or departing for the day).

6. At the end of the day, all files containing PII are to be returned to the locked filing cabinet by department heads or the Data Security Coordinator.

7. Paper or electronic records containing PII shall be disposed of in compliance with M.G.L. c. 93I (Standards for disposal of records containing personal information; disposal by third party; enforcement). Paper and electronic media documents containing PII shall be either redacted, burned, pulverized or shredded so that PII cannot be read or reconstructed.

8. Electronic records containing PII shall not be stored or transported on any portable device, sent or transmitted, unless they are encrypted.

9. If necessary, for the functioning of individual departments, the department head, in consultation with the Data Security Coordinator or Information Security Committee, may develop department rules that restrict access and handling of files containing PII, which must comply with all WISP requirements. Department rules are to be published as an addendum to the WISP.
Third-Party Service Providers

Any service provider or individual that receives, stores, maintains or processes PII or is permitted access to any file containing personal information ("Third-Party Service Provider") is required to meet the following security requirements, as well as any and all standards of 201 CMR 17.00. Examples include third parties who provide offsite backup storage copies of all GCC electronic data; paper record copying or storage service providers; and contractors or vendors working with customers with authorized access to GCC records.

- Any contract with a Third-Party Service Provider signed on or after March 1, 2010 shall require the Service Provider to implement security standards consistent with 201 CMR 17.00.
- The Data Security Coordinator is responsible for obtaining reasonable confirmation that any Third-Party Service Provider is capable of meeting security standards consistent with 201 CMR 17.00.
- Any existing contracts with Third-Party Service shall be reviewed by the Data Security Coordinator and/or the Information Security Committee. These Service Providers shall meet the security standards consistent with 201 CMR 17.00 by an agreed-upon date, or other Service Providers will be selected, when feasible to do so.
- A list of currently known third-party service providers who have access to the Greenfield Community College IT environment(s), sensitive information, or PII shall be maintained by the Data Security Coordinator.

Information Incidents

When any student or member of the Greenfield Community College workforce (including Third-Party Service Providers) learns of a security breach, for instance: If an unencrypted laptop has been lost, stolen or accessed without authorization; or an encrypted laptop along with the access code has been acquired by an unauthorized person, the following process shall be performed:

1. Notify the Data Security Coordinator or department head about a known or suspected security breach or an unauthorized use of personal information.
   a. Laura Garcia (413-775-1318 or GarciaL@gcc.mass.edu)

2. The Data Security Coordinator shall work with the Information Security Committee to draft a security breach notification to submit to the Massachusetts Office of Consumer Affairs and Business Regulation, the Massachusetts Attorney General’s office, and any others deemed necessary by another State or Country Breach Notification law, as appropriate. The security breach notification shall include:
   a. A detailed description of the nature and circumstances of the security breach or unauthorized acquisition or use of personal information;
   b. The number of Massachusetts residents affected at the time the notification is submitted;
   c. The steps already taken relative to the incident;
   d. Any steps intended to be taken subsequent to the filing of the notification, and;
   e. Information regarding whether law enforcement officials are engaged in investigating the incident.
Policy Compliance

Violations, deliberate or inadvertent, may result in disciplinary actions, up to and including termination and legal action. As with all disciplinary matters, principles of fairness and equity always apply.