PERSONALLY IDENTIFIABLE INFORMATION POLICY

I. Policy Section

15.0 Information Technology

II. Policy Subsection

15.1 Personally Identifiable Information

III. Policy Statement

It is the policy of GRCC to protect personally identifiable information (PII) of employees and students. The electronic restrictions and safeguards outlined in this policy provide guidance for students, employees, and contractors that have access to PII retained by the College to ensure compliance with state and federal regulations.

IV. Reason for Policy

To ensure that anyone that collects or uses PII at GRCC does so in compliance with state and federal regulations and best practices for information security in higher education.

V. Entities Affected by this Policy

This policy will affect students, employees, and contractors that have been granted access to resources containing PII.

VI. Who Should Read this Policy

Students, Employees, and Contractors

VII. Related Documents

Family Education Rights to Privacy Act (FERPA)
Health Insurance Portability and Accountability Act
(HIPAA) Payment Card Industry Data Security
Standard (PCI-DSS) Gramm–Leach–Bliley Act
(GLBA)
GRCC Acceptable Use Agreement
(AUA) Red Flags Rule
Freedom of Information Act

VIII. Contacts

Policy Owner: Chief Information Officer
Information Security Officer
Information Security Analyst
HIPAA Security Officer
Registrar/FERPA Security Officer

IX. Definitions

A. Personally Identifiable Information (PII) - is any information pertaining to an individual that can be used to distinguish or trace a person's identity. Some information that is considered PII is available in public sources such as telephone books, public websites, university listings, etc. This type of information is considered to be **Public PII** and includes:

1. First and Last name
2. Address
3. Work telephone number
4. Work e-mail address
5. Home telephone number
6. General educational credentials
7. Photos and video

In contrast, **Protected PII** is defined as any one or more of types of information including, but not limited to:

1. Social security number
2. Username and password
3. Passport number
4. Credit card number
5. Clearances
6. Banking information
7. Biometrics
8. Mothers maiden name
9. Criminal, medical and financial records
10. Educational transcripts
11. Photos and video including any of the above

(If a question arises about what is or isn't PII please contact the Information Security Department at it_security_team@grcc.edu)

B. GRCC Information System - A collection of computing resources that are accessible through privileged access such as a login or key. Usually a software package designed to store student and employee data. E.g. PeopleSoft, Blackboard, TutorTrac, and Eaglesoft.

C. Secure Deletion - Secure deletion of an electronic file is accomplished by overwriting the full file contents with random data multiple times.

X. Procedures

A. General

This section provides guidelines on how to maintain and discard PII. If current procedures fall outside this policy or questions arise please contact the Information Security Department to suggest more efficient procedures for protecting PII.

All electronic files that contain Protected PII will reside within a protected GRCC information system location. All physical files that contain Protected PII will reside within a locked file cabinet or room when not being actively viewed or modified. Protected PII is not to be downloaded to personal or college owned student, employee, or contractor workstations or mobile devices (such as laptops, personal digital assistants, mobile phones, tablets or removable media) or to systems outside the protection of the college. PII will also not be sent through any form of insecure electronic communication E.g. E-mail or instant messaging systems. Significant security risks emerge when PII is transferred from a secure location to a less secure location or is disposed of improperly. When disposing of PII the physical or electronic file should be shredded or securely deleted. For help with secure deletion please contact the Information Security Department at it_security_team@grcc.edu.

B. Exceptions

If there is an operational or business need to store protected PII outside a GRCC information system please contact the Information Security Department at it_security_team@grcc.edu for assistance in securing the information.

C. Incident Reporting

The Information Security Department must be informed of a real or suspected disclosure of Protected PII data within 12 hours after discovery. E.g. Misplacing a paper report, loss of a laptop, mobile device, or removable media containing PII, accidental email of PII, possible virus, or malware infection or a computer containing PII.

D. Audits

Periodic audits of GRCC owned equipment and physical locations may be performed by the Information Security Officer or delegates to ensure that protected PII is stored in approved information systems or locations. The purpose of the audit is to ensure compliance with this policy and to provide information necessary to continuously improve business practices.

XI. Enforcement

An employee found to be in violation of this policy may be subject to disciplinary action as deemed appropriate based on the facts and circumstances giving rise to the violation.

XII. Forms

N/A

XIII. Effective Date

October 16, 2012

XIV. Policy History

December, 2014 - revised policy and incorporated new format
September, 2018 - removed “date and place of birth” from protected PII section

XV. Next Review/Revision Date

December, 2022