Information Security Breach Reporting and Notification Policy
Approved by the President on 2/9/09

1. General

Golden Gate University values individuals' privacy and actively seeks to preserve the privacy rights of those who share information with us. GGU is dedicated to preventing unauthorized information access, maintaining information accuracy, and ensuring the appropriate use of information. We strive to put in place appropriate physical, electronic, and managerial safeguards to secure the information we collect in all formats: on paper, electronically, and verbally.

This policy provides procedures for responses to:

- known or suspected information security breaches,
- disruptions caused by the failure of a security mechanism, and
- known or suspected security incidents.

This policy provides guidance on documenting the incident, determining notification requirements and working with GGU administration to remediate any damage.

Mitigation or notification requirements may differ, depending on federal or state statutes, the nature of the information at risk in the event of a security breach, or contractual agreements. Under California law, notification obligations extend only to California residents. However the University will make reasonable efforts to extend notification to affected out of state residents as well. There may also be specific notification requirements that relate to GGU’s contractual relationships with third parties.

2. Reporting Requirements

Any member of the University community, students, faculty and staff, who believe there has been an information security breach shall report this to their supervisor who must immediately report the potential breach to the Office of the President or the Vice President for Academic Affairs.
3. **Notification in Instances of Security Breaches Involving Electronic Personal Information**

Notice of a security breach must be given following discovery or notification of a breach in the security of the computerized data when the unencrypted personal information of a California resident was, or is reasonably believed to have been, acquired by an unauthorized person.

The definition of “personal information” is:

An individual’s first name or first initial, and last name, in combination with any one or more of the following:

- social security number
- driver’s license number or California identification card number
- account number for a financial account, 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
- medical information, meaning any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.
- health insurance information, meaning an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.
- Good faith acquisition of personal information by a University employee or agent for University purposes does not constitute a security breach, provided that the personal information is not used for or subject to further unauthorized disclosure.

4. **Notification Procedures**

In the case of a security breach as defined in this section, GGU shall follow the procedures here to provide notification of the breach to those individuals whose personal information is reasonably believed to have been acquired by an unauthorized person.

Notification must occur in the most expedient time possible and without unreasonable delay, except:

- when a law enforcement agency has determined that notification will impede a criminal investigation (in this case, notification must occur as soon as the law enforcement agency determines that it will not compromise the investigation) or
- when necessary to discover the scope of the breach and restore the integrity of the system.
5. **Method of Notification**

The Office of the President and / or the Vice President for Academic Affairs or their designee shall determine the language to be used in the notification, which may be distributed by one of the following methods:

- written, hard copy notice or
- e-mail notice.

Telephone communication or other timely communication to an individual’s representative may be used when it is determined that written notice may adversely affect a patient’s health.

If sufficient contact information is not available for direct hard copy or e-mail notice, a substitute method of notice may be used. Substitute notice shall include prominent display on the University’s Web site or other commonly used Web site for at least forty-five days. The Office of the President and / or the Vice President for Academic Affairs or their designee shall determine the language to be used in the substitute notice. The University may provide notification to affected individuals if personal information beyond the data elements defined here is reasonably believed to have been acquired by an unauthorized person.

Any written communications involving legal counsel should assert attorney-client privilege to ensure strict confidentiality, as appropriate.