# GOLDEN STATE COLLEGE OF COURT REPORTING & CAPTIONING

## *INFORMATION SECURITY POLICY*

Golden State College (GSC) is committed to respecting and protecting the security and privacy of information assets entrusted to the college. The unauthorized collection, processing, modification, deleting, or disclosure of information in college files and data bases can disrupt college operations, compromise the integrity of the college program, violate individual rights to privacy, and constitute a criminal act.

This policy supports the mission of the college by protecting the college's information resources, reputation, legal position, and ability to conduct its operation. The term "information" is used as a general terms and includes data stores and databases. The purpose of this policy is to protect the interests of those college constituents who rely on information and the systems and communications that deliver the information, from harm resulting from failure of availability, confidentiality and integrity.

These security measures shall be considered to be met when...

1. (Availability) ...Information is available and usable when required, and the systems that provide it can appropriately resist attacks and recover from or prevent failures
2. (Confidentiality)...Information is observed by or disclosed to only those who have a right to know;
3. (Integrity) ...Information is complete, accurate and protected against unauthorized modification;
4. (Authenticity)...Business transactions, as well as information exchanges, can be trusted.

The Information Security Policy of Golden State College is intended to

1. Provide direction on developing and implementing protection measures that establish accountability and prudent and acceptable practices regarding the use and safeguarding of campus information assets;
2. Protect the privacy of personally identifiable information entrusted to the college;
3. Ensure compliance with applicable GSC policies, state and federal laws, and regulations regarding the management and security of information assets; and
4. Educate individual users and business associates with respect to their responsibilities associated with the use of university information assets.

---

Information security and risk management are based upon an appropriate division of responsibility among management, administrative and program staff. Every employee and business associate that comes in contact with college data is held accountable for his/her actions. Individuals and business associates, who have been granted access to college

resources, are responsible for adhering to the provisions of this policy to ensure that the confidentiality, integrity, and availability of GSC information are maintained in accordance with applicable GSC policies, federal and state statutes, and regulations, and industry best practices governing information security.

All information entrusted to GSC is considered an information asset, and, as such, every employee or business associate that collects, stores, processes, transfers, administers, maintains, or disposes of an information asset owned or entrusted to the college is responsible and held accountable for its appropriate use.

---

The Board of Directors of Golden State College, the Chief Executive Officer, and the campus management team actively support the development and implementation of the campus information security policy and the campus information security program. This support is demonstrated through clear direction, commitment and acknowledgement of information security roles and responsibilities.

The School Director is responsible for coordinating activities related to information security, including appropriate protection from loss, inappropriate disclosure, and unauthorized modification.

---

Social Security Numbers (SSNs)

GSC recognizes the special risks associated with the collection, use and disclosure of social security numbers. Therefore, the requirements of this policy apply to all social security numbers contained in any medium, including paper records.

If the collection or use of social security numbers is permitted, but not required by applicable law, the college shall use and collect social security numbers only as reasonably necessary for the proper administration or accomplishment of educational, business, and governmental purposes.

Documents, such as Enrollment Agreements, that bear a student's SSN shall be locked by key in a fireproof file drawer, accessible only to appropriate personnel.

---

Credit Card, Bank Account Information

Golden State College has established rules for the protection of payment card (credit and debit cards) information. The major credit card companies (Visa, Master Card, Discover, American Express) established the Payment Card Industry Security Standards Council to promote wide adoption of the payment card industry data security standard (PCI DSS or PCI). This standard establishes rules for the protection of payment card information. GSC credit card practices are in compliance with the PCI standards.

---

Access to information should be controlled on the basis of business and security requirements. Procedures to manage access to college assets, including confidential/sensitive data and critical applications, must be documented.

The School Director is responsible for processing requests to access operational systems, such as Diamond D, the campus management software.

In no event will students or other non-employees be granted access to critical systems or sensitive/confidential college information.

Employees may only access critical assets or confidential/sensitive data, if access is required to perform their duties. However, the School Director must approve such access before access is granted. If the School Director denies access to the desired protected information, access will not be granted.

---

The college recognizes that business associates serve an important function in the support of services, hardware and software. Business associates must comply with all applicable college policies, standards, business practices, and all federal and state laws to which GSC must adhere to ensure that the college remains in compliance with such policy or law.

The School Director is responsible for managing business associates' access to sensitive, confidential or critical college assets.

Access to the campus network shall be managed to ensure that network services are not compromised. The college will install appropriate interfaces between the campus network and the internet or networks owned by other organizations. Appropriate authentication mechanisms will be used to manage access to areas or devices on the network that store critical applications or confidential/sensitive materials. Users shall access network resources or services that they have been specifically granted authority to use.

Users are required to comply with the Acceptable Computer Use Policy. The college maintains processes to enforce safe wireless access.

---

The process for logging into operating systems shall be designed to minimize the opportunity for unauthorized access. All users shall be assigned a unique identifier (user ID) for their personal use only, and a suitable authentication technique shall be chosen to substantiate the claimed identity of a user.

Under special circumstances, where there is a clear benefit to the college, the use of a shared user ID for a group of users or a specific job can be used. Approval by the School Director is required in such cases.

Generic IDs for use by an individual shall only be allowed either where actions carried out by the ID do not need to be traced (for example, read-only access), or where there are other controls in place (for example, password for a generic ID only issued to one staff at a time and logging such instance). Exceptions to this requirement may be granted with approval from the asset owner and the School Director.

---

Directories or Lists: Any directory application that provides access to information collected by GSC about individuals must adhere to all applicable privacy laws. Such laws may allow individuals to establish privacy preferences. For example, Family Educational Rights and

Privacy Act (FERPA) blocks allow a student to limit the disclosure of their directory or listed information.

---

Acceptable Computer Use Policy: All users are required to follow the college's Acceptable Computer Use Policy which defines acceptable and unacceptable computing uses and practices at the college. College employees who have access to confidential information are required to properly protect and not distribute the data in a way that compromises its confidentiality.

---

Users must log off from applications, computers, and networked device when finished. Users, who hold accounts that grant access to critical applications or confidential/sensitive data, must not leave their workstations or storage devices (i.e., PDA, flash drives, CD/DVDs, portable hard drives) unattended. If computers are located in a public or shared area, users must complete their session and log off completely before leaving their computer.

Users must not leave workstations, fax machines and other devices that contain confidential/sensitive data unattended.

---

When donating, selling, transferring, or disposing of computers or removable media, care must be taken to ensure that critical systems or confidential/sensitive data is rendered unreadable. Users must follow the guidelines issued by the School Director in conjunction with the IT (Information Technology) provider for donating or transferring equipment that is no longer needed.

---

In the case of a declared disaster, the security and availability of confidential information will be through a combination of the back-up program Carbonite and the asset owner.

---

When acquiring software, the software must be used in accordance with the applicable software license. All software installed at GSC must be acquired from a reputable source that will accept responsibility for its integrity. The operational requirements of new systems and changes to the operational requirements of existing systems should be discussed and documented in the early stages of a project. These requirements must consider the administrative, technical and physical controls needed to protect the confidentiality, integrity, and availability of the information system.

---

Information Technology resources and services provided via the GSC-hosted Web site to the GSC community or to the public must adhere to established technology accessibility guidelines and law, including Section 504 of the Rehabilitation Act of 1973 and the American Disabilities Act (ADA) of 1990.

The college's network infrastructure and other information resources must be continuously protected from known vulnerabilities and threats posed by computer viruses, worms, and other types of hostile computer programs. All GSC devises that connect to the campus network must run recommended current virus protection software and adhere to any other protective measures as required by applicable policies and procedures.

If students, staff or technical staff detect signs of malicious code affecting the college's infrastructure, it should be reported to the School Director.

---

Destruction and disposal of information and devices containing critical systems or confidential/sensitive information must be handled in a manner as to ensure confidential/sensitive data cannot be retrieved and recovered by unauthorized persons.

Whenever authorized users print confidential/sensitive information, they are responsible for properly disposing of the printed information, once it is no longer required. Confidential/sensitive information assets shall be retained in a secure environment before being released to authorized individuals for appropriate disposal.

---

Confidential or sensitive information is housed in secure areas that are protected from unauthorized physical access or damage. These secure areas are protected by appropriate entry controls, and are protected against damage from man-made, environmental, accidental, or natural disasters.

The primary protection against intentional risks such as theft, intrusion, or vandalism is vigilant observation by the GSC community and adherence to policies related to the securing of equipment and locking of files when not utilized and firm control of access by means of account and passwords and access limits. Employees must notify the School Director when they discover an incident of theft, vandalism or sabotage.

Office administrative staff is responsible for ensuring that all security procedures within their area of responsibility are carried out to achieve compliance with campus information security policies and standards.

Information security events should be reported through appropriate management channels as quickly as possible. All employees and business associates who have been given access to information assets entrusted to GSC or utilize college services must report observed or suspected security weaknesses in systems or services to the School Director.

Any member of the campus community who has evidence that college information has been accessed without proper authorization or detects suspicious activity that could potentially expose, compromise or destroy information entrusted to GSC must report these incidents to one

of the school owners or the School Director.  No one should take it upon himself or herself to investigate or remediate the matter.

Members of the campus community who observe information security violations may also report them anonymously by directly contacting one of the school owners or the School Director.

---

Enforcement

It is the responsibility of all faculty, staff and students to report any suspected or confirmed violations of this policy to the School Owners or the School Director.  Members of the campus community who observe information security violations may report them anonymously by contacting the School Owners or the School Director.

Employees who fail to adhere to this policy may be subject to penalties and disciplinary action, both within and outside the college.  Violations will be handled through applicable college disciplinary procedures.

A violation of this policy by business associates may result in penalties and disciplinary action, both within and outside the college.  Violations will be handled through applicable college disciplinary procedures and may include terminating the work engagement.

Students who violate this policy may be referred to the School Director and handled through applicable college disciplinary procedures under the Student Code of Conduct.

The college may temporarily suspend, block or restrict access to resources, independent of such procedures, when it reasonable appears necessary to do so in order to protect the integrity, security, or functionality of college resources or to protect the college from liability. The college may also refer suspected violations of applicable law to appropriate law enforcement agencies.

---