

Glossary of GC IT Policy-Related Terms

Confidential Information : The term *confidential information* applies broadly to information for which access or disclosure may be assigned some degree of sensitivity, and therefore, for which some degree of protection or access restriction may be warranted. Unauthorized access to or disclosure of information in this category could result in a serious adverse effect, cause financial loss, cause damage to the College's reputation and loss of confidence or public standing, constitute an unwarranted invasion of privacy, or adversely affect a partner, e.g., a business or agency working with the College.

Electronic Information Resource (EIR) : A resource used in support of College activities that involves the electronic storage, processing or transmitting of data, as well as the data itself. Electronic Information Resources include application systems, operating systems, tools, communications systems, electronic services, including services offered through contracts with the College, data in raw, summary, and interpreted form; and associated computer servers, desktops (workstations), portable devices (laptops, PDAs) or media (CD ROM, memory sticks, flash drives), communications and other hardware used to conduct activities in support of the College's mission. These resources are valued information assets of the College.

Personal Identity Information (PII): Personal identity information (PII) is the electronic manifestation of an individual's first name or first initial, and last name, in combination with one or more of the following:

- Social Security number (SSN)
- Drivers license number or State-issued Identification Card number
- Account number*, credit or debit card number in combination with any required security code, access code, or password that could permit access to an individual's financial account
- Medical information, including 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, including 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

This definition of electronic PII is not dependent on where the personal identity information is stored. This includes, but is not limited to, formal database systems such as CAMS, Dynamics GP, or GreenEmployee as well as simple text files, spreadsheets, etc. Electronic personal identity information may exist on, but is not limited to, hard drives, magnetic tape, optical disks, diskettes, hand held computing devices, etc.

**Note: “Account number” is not defined in the legislation but can refer to any financial account such as a bank or brokerage account, etc*

Restricted data or information : Any confidential or personal information that is protected by law or policy and that requires the highest level of access control and security protection, whether in storage or in transit. At GC, restricted data includes, but is not necessarily limited to:

- **Personal Identity Information (PII)**
 - Electronic protected health information (ePHI) protected by Federal HIPAA legislation
 - Credit card data regulated by the Payment Card Industry (PCI)
 - Passport number
 - Passwords providing access to restricted data or resources
 - Information relating to an ongoing criminal investigation
 - Court-ordered settlement agreements requiring non-disclosure
 - Information specifically identified by contract as restricted
 - Other information for which the degree of adverse affect that may result from unauthorized access or disclosure is high
-

Subject Matter Expert (or Data Expert): A Subject Matter Expert (SME) is the individual or unit responsible for advising on the appropriate use, protection, access, degree of sensitivity, criticality, and risk tolerance of a specific data set. A SME can be, but is not necessarily, the System Steward for that data set. Integrated data typically has multiple SMEs.

System Steward (also known as the Electronic Information Resource Proprietor; Data, Resource, or Record Proprietor; Data Steward; or Data Owner): The individual with ultimate responsibility for a defined set of College electronic information, including determining who should have access to it, and ensuring that the information is protected adequately and is used in ways consistent with the mission of the College as a whole. This can be, but is not limited to, the operating head of a unit or a designee.