**Policy**

The California State University (CSU) protects the privacy of our faculty, staff, students, alumni, and other individuals who interact with the university through the following pursuant to the principles listed below. All CSU employees share the responsibility to safeguard and collect only what is necessary for legitimate business purposes and in accordance with these principles:

* CSU **privacy governance** is provided by designated university and chancellor’s office CSU Data Privacy Officers who collaborate systemwide to assess privacy risk, prioritize privacy initiatives, and develop and implement common policies and procedures to collect, use, store, and when necessary, disclose personal data.
* CSU **privacy** **objectives** are to ensure data accuracy, collect and disclose data only for necessary purposes and integrate data minimization and privacy by design into operational practices.
* CSU **privacy** **processes**obtainpersonal, sensitive, and protected data lawfully with transparent communication to individuals about the purpose of collecting their data and how their data is used for specified purposes. Technical and organizational measures secure data, and data retention aligns with the CSU Records Retention Policy for secure disposal.

**Definitions**

* **Personal Information** - Personal information refers to any information that can be used to identify, relate to, describe, or be associated with a particular person or household. It includes a wide range of information, such as name, address, phone number, email address, social security number, driver's license number, passport number, IP address, biometric data, and any other information that could reasonably be linked to a particular individual or household.
* **Sensitive Information** - Personal information that reveals a person’s government identifier, financial account in combination with any required access credentials, precise geolocation, racial or ethnic origin, religious or philosophical beliefs, union membership, contents of electronic messages unless the business is the intended recipient of the communication, unique genetic and biometric information, information related to a persons’ health, sex life or sexual orientation.
* **Protected Information** - Protected information means any characteristics of protected classifications under California or federal law (e.g., HIPAA, FERPA). Examples include age, marital status, medical condition, gender, veteran, or military status.
* **Data Privacy Officers** - designated individuals within the CSU who oversee the data privacy implementation to ensure compliance with applicable laws, regulations, policies, and principles related to data privacy. Data privacy officers may oversee specific areas (e.g., HIPAA, FERPA) or may focus on organizational strategy to enhance data privacy.
* **Data Owner** - Senior-level leader or executive who has ultimate accountability for specific data sets or assets.
* **Data Custodian/Steward** - Individual who is responsible for complying with applicable laws and policies. Manage and maintain the quality, and security of a specific dataset. Notify privacy officer of privacy risks and work with privacy officer to mitigate risks.

**Procedure**

CSU campuses and the Chancellor's Office shall collaborate to develop and maintain common operational procedures guided by the [National Institute of Standards and Technology (NIST) Privacy Framework](https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf) encompassing the core privacy functions – identify, govern, control, communicate and protect.

* Use the NIST Privacy Framework to assess the institution’s privacy practice maturity, risk profile and prioritize privacy initiatives.
* Build and foster a culture that balances the open nature of higher education with the importance of data privacy and building stakeholder trust consistent with CSU’s risk tolerance.
* Fulfill applicable compliance obligations.
* Facilitate communication and awareness about privacy practices with internal and external stakeholders.
* Promote privacy program collaboration with information security teams, data owners and data stewards.
* Utilize a common language when discussing privacy in our organization.
* Plan and implement privacy processes.
* Train employees.
* Measure outcomes against goals.

The system will utilize a common privacy platform and approach to facilitate and support privacy processes.

**Guidelines**

The following recommendations should be considered when implementing the policies and procedures provided above.

**National Identifiers**

Before we collect national identifiers linked to an individual (such as a government issued social security number or tax identification number), here are some guidelines to validate the necessity to collect or process the data. If we can reasonably achieve the same result in another less intrusive way these would not apply:

1. Fulfilling a contract in which the data subject is part of to take steps at the request of the data subject (like paying a vendor)
2. Fulfilling a legal obligation (like payroll tax reporting)
3. Tasks carried out in public interest (like disbursing federal financial aid to our students)
4. Tasks carried out in vital interest (like emergency medical care provided by first responders, and they notate in their record that the patient resuscitated is wearing a medical alert bracelet with a specific diagnosis)
5. Criminal offense (if there has been a criminal offense, the campus public safety department would therefore have specific data they need to collect related to the offense)
6. Legitimate interest. In general, the condition applies when *all* the following apply:
	1. Purpose - there is a legitimate interest behind collection/processing that data
	2. Necessity – the collection/processing is necessary for that purpose
	3. Balancing – if the interest does not override the individual’s interests, rights or freedoms
7. When the data subject consents to provide that information. With this item, best practices are to implement a consent module to document the data subject’s consent.

Collection of national identifiers for validation of identity to provision account access is not considered a valid reason for collection and processing of national identifiers.

**Sale of Data**

While our necessity to sell data would be extremely limited, we should review the following guidelines before doing so to validate the necessity:

1. Do not sell information collected or processed to third parties that exceeds the initial purpose of collection or processing without documented consent from the data subject.
2. Data subjects may revoke consent and therefore we must stop the sale or sharing of information with a third when consent is revoked.
3. Data subjects may request that we delete their information that was shared with third parties and therefore it is best to not sell or share information that is not necessary to collect.

**References**

* [California Code of Regulations, 5 CCR § 42396](https://govt.westlaw.com/calregs/Document/I5A2F29434C6911EC93A8000D3A7C4BC3?viewType=FullText&originationContext=documenttoc&transitionType=CategoryPageItem&contextData=(sc.Default)&bhcp=1)
* [Systemwide Records Information Retention and Disposition Schedules Implementation Policy](https://calstate.policystat.com/policy/6594392/latest)
* [Designation of Health Care Components for Purposes of the Health Care Portability and Accountability act of 1996](https://calstate.policystat.com/policy/6591918/latest)
* [Privacy and Personal Information Management Student Records Administration](https://calstate.policystat.com/policy/8609851/latest)
* [CSU Information Security Policy and Standards](https://calstate.policystat.com/policy/11773867/latest#autoid-jvmyn)
* CSU InfoSec Data Classification Levels

**Authority**

This policy is issued pursuant to [Section II of the Standing Orders of the Board of Trustees of the California State University](https://calstate.policystat.com/policy/6593385/latest/#autoid-46jr3) as further delegated by the [Standing Delegations of Administrative Authority](https://calstate.policystat.com/policy/7646754/latest/). The president may delegate authority and responsibility described in this policy to other university officials pursuant to [Section VI of the Standing Orders of the Board of Trustees of the California State University](https://calstate.policystat.com/policy/6593385/latest/#autoid-46jr3).