**Protection of Computerized Personal Information Procedure**

The **[Organization]** is responsible for safeguarding of any personal data about its employees and contractors. It is also responsible for maintaining compliance with the Family Educational Rights and Privacy Act (FERPA) with regards to student data.

# PurposeThe purpose of this procedure is to implement the requirements needed to enhance the management of personal information that could be used, possibly in conjunction with other information, to impersonate an individual in ways that might cause serious loss of privacy, financial damage, and/or violate regulations about the protection of such data.

# Scope

# All computing systems owned by [Organization], any protected data on [Organization] systems, and any data where an [Organization] employee is considered the data custodian, are subject to this procedure.

# Procedure

Each department is urged to create their own procedures to limit the collection, distribution, and retention of personally identifying electronic data to ensure that the data that is retained is critical to their business needs and that anything outside of that is securely destroyed.

Best practice guidelines for departments include:

* Collecting and retaining only that data which is essential to the performance of assigned tasks
* Deleting personal information when there is no longer a business need for its retention on computer systems
* Providing staff access to sensitive data only as needed to perform assigned duties
* Designing database systems so that personal information can be identified
* Notifying receivers when personally identifying information is included in the distribution of data to any downstream users, including references to the guidelines
* Redacting personal information not critical to the task when distributing full data sets to downstream users
* Configuring electronic applications that check authorizing or authenticating databases to return confirming responses rather than personal information (whenever possible)
* Reviewing and updating agreements with external service provides to ensure vendor compliance with these requirements
* Preparing in advance, in the event of, the need for any immediate notification to individuals whose personal data is retained on computing systems
* Never leaving sensitive data exposed on computer screens when not in use, and never leaving computer screens unattended without appropriate screen access controls

In the event a breach is suspected, the following Incident Response Process will be enacted.

1. If a breach is suspected on a computing system that contains or has network access to unencrypted protected data, the Data Custodian must immediately:
* Remove the computing system from the network
* Alert the Cybersecurity Team and the Incident Response Team, and allow them to conduct local analysis of the breach
* Notify the Data Owner if there is a reasonable belief that protected data may have been acquired
1. Under advisement of the Cybersecurity Officer, the Incident Response Team will examine the evidence of a breach with the Data Custodian to assess the possibility that protected data has been obtained.
2. The Incident Response Team will notify the Cybersecurity Officer if there is a possibility that protected data has been acquired by an unauthorized source.
3. Depending upon the situation, law enforcement should be notified by the Cybersecurity Officer.
4. The Data Custodian must report to the Data Owner the number of individuals whose protected data may have been acquired.
5. If, after continued analysis, the Incident Response Team and the Data Custodian have sufficient reason to believe that protected data may have been acquired, the Data Custodian will submit a report to the Cybersecurity Officer that includes:
* The nature of the security breach, including data, time of breach, and detection
* The number of individuals affected, including contact information
1. The Cybersecurity Officer will assign a Cybersecurity Analyst to oversee the breach investigation, response, and remediation requirements. The Cybersecurity Officer will make the determination if notification under California Civil Code 1798.29 and 1798.82 is required and will notify the Data Owner. The Data Owner retains responsibility for all aspects of notification.
2. Notification should include all of the following information:
* The date(s) on which the personal information was (or could have been) acquired
* A description of the personal information which was (or could have been) acquired
* The name of the department or unit responsible for the information and the relationship that the affected individual has (had) to the department
* An indication of the likelihood that the personal information was acquired or used
* A list of resources that affected individuals could use to check for potential misuse of their information
* An email address and phone number of a suitable department representative with sufficient knowledge of the incident to be able to handle questions from affected individuals

Responsibilities

* **Lead Authority** is responsible for:
* Ensuring that the incident response process if followed
* Ensuring that notification procedures are followed
* Coordinating procedures with counsel as appropriate
* **Cybersecurity Officer** has oversight responsibility for:
* Ensuring that Data Owners develop adequate security plans for computing systems within their jurisdiction
* Ensuring that Data Owners develop adequate procedures for access to protected data
* Ensuring that Data Custodians conduct an inventory of computing systems under their jurisdiction
* Determining which computer system contains protected data or have access to protected data that are subject to these requirements
* Ensuring the collection of email or postal address information for any individuals for whom protected data is retained (for notification purposes)
* Conducting an annual review of control records and updating them as necessary
* Establishing an immediate notification plan, including boiler plate text, which can be implemented in the event of a breach that would have immediate impact on individuals whose personal information may have been obtained by a non-authorized source
* **Data Owners** are responsible for:
* Creating and maintaining control records identifying computing systems containing unencrypted protected data as defined within this procedure
* Ensuring the development of adequate security measures consistent with existing **[Organization]** standards/procedures
* Establishing procedures to ensure that all staff, within their jurisdiction, who have access to or make use of protected data, abide by **[Organization]** procedures regarding protected data
* Maintaining control records in a secure environment
* **Data Custodians** must:
* Implement adequate security measures for computing systems containing protected data within their jurisdiction
* Implement appropriate encryption strategies for both the transmission and storage of protected data
* Establish adequate procedures to indicate if unauthorized access to or anomalous activity occurs on computing systems. Data Custodians may consult with Network or Cybersecurity for assistance in determining strategies appropriate to their technological environment.
* Establish procedures to monitor access to computing systems which house protected data
* **Data Users** must:
* Abide by established procedures on access to and use of protected data
* Protect the resources under their control, such as, access passwords, computers, and the data that they download

# Enforcement

This procedure is for your protection. Violation of this procedure could be reported to the appropriate supervisor and be subject to potential disciplinary action, up to and including termination.

# Exceptions

Limited exceptions to the procedure must be approved by the **[management]**.

1. **Definitions**
* Computing System: Any server, desktop, laptop computer, or mobile device (including smartphones) that contains or provides access to protected data.
* Control Records: A database, spreadsheet, or any other electronic file that contains a list of computing systems that contain protected data. Control records must contain the following:
* Name of computing system Data Custodian
* Physical location of computing system
* Description of logical access and security controls
* Protected Data: The data comprising personal information governed by these guidelines is defined as protected data. This protected data includes an individual’s first and last name in combination with any of the following:
* Social security number
* Driver’s license or identification card number
* Financial account or credit card number
* Medical information
* Health insurance information
* Student data