Last Revised: **November 11th, 2024**

BERKELEY COLLEGE

DATA SECURITY POLICY

BERKELEY COLLEGE
DATA SECURITY POLICY

TABLE OF CONTENTS

CHAPTER 1 – INTRODUCTION

Accurate, timely, relevant, and properly protected information is a critical asset of Berkeley College. The College is committed to ensuring that sensitive College information is protected from unauthorized access or disclosure. The College recognizes that failure to implement adequate security controls over sensitive College information could potentially lead to:

1. Irretrievable loss of important data;
2. Loss of data integrity or reliability;
3. Serious financial consequences;
4. Damage to the reputation of the College; and/or
5. Legal penalties.

Measures must be in place to minimize the risk to the College from unauthorized disclosure of sensitive College information, whether accidental or deliberate. To comply with data protection laws, sensitive College information must be collected and used appropriately, stored safely, and not disclosed to any other person unlawfully.

The object of this Data Security Policy is to define the security controls necessary to safeguard the confidentiality, integrity, and availability of sensitive College information. This policy provides a framework in which security threats to College information systems, both digital and physical, can be identified and managed on a risk basis and establishes terms of reference which ensure uniform implementation of data security controls throughout the College.

Scope:

This Data Security Policy applies to all associates (including Federal Work Study students), vendors, agents, consultants, contractors, or any other authorized party who has access to College Data. Failure to comply may result in loss of data access privileges and possible disciplinary action, up to and including termination, as well as potential legal consequences. Further, in the case of lost, damaged, or stolen College-owned equipment caused by an associate's willful negligence or intentional misuse, the College may seek reimbursement from the associate to cover the cost of repair or replacement.

Authority:

This Policy authorizes Berkeley College's Information Systems Department to develop and implement a comprehensive program of data security policies, directives, procedures, and controls to ensure protection of sensitive College information and compliance with applicable policies, laws, and regulations. In order to accomplish these goals, the Information Systems department may utilize additional resources and personnel as required from other College departments or authorized third parties.

CHAPTER 2 – GENERAL ROLES AND RESPONSIBILITIES

A. **Functional Vice Presidents** are responsible for establishing and implementing internal controls to ensure that all members of their department(s) comply with this policy. Functional Vice Presidents are also responsible for designating a Data Steward for all data systems under their control.

B. **Data Stewards** are designated by their department's Functional Vice President and are responsible for the following:

   1. Security Policies and Procedures. Data Stewards are responsible for establishing the procedures related to the creation, retention, distribution, training, and disposal of information under their control and supervision. These must be consistent with this policy, other College policies, contractual agreements, and Federal and state laws and regulations. Data Stewards may impose additional requirements that enhance security with more specific data security policies and procedures for their information where appropriate.

   2. Authorizations. Data Stewards determine who is authorized and approved to view, edit, or otherwise modify College Data. They shall make sure that Users have a legitimate need to know the information and understand the sensitivity and security requirements of that information.

   3. Annual Security Procedure Reviews. Data Stewards must meet with their two (2) designated Access Administrators at least annually to review security procedures, user roles, and perform a user entitlement review.

   4. Vacant Data Steward Positions. If a Data Steward position becomes vacant for any reason, the responsible Functional Vice President will serve as the Data Steward until the position is filled.

C. **Access Administrators** are designated by the Data Steward. Access Administrators are responsible for controlling access to College data systems by granting or denying access rights to Users at the direction of the Data Steward and the Human Resources Department. If one of the Access Administrator position becomes vacant and no alternate is available, the Data Steward will act as the secondary Access Administrator until a new Access Administrator can be assigned

D. **Users** means any person who has access to College Data. Users are responsible for protecting College Data to which they have access. Their responsibilities cover both digital and physical information. This also includes all technology devices in their possession, whether College owned or personally owned, that contain College Data.

E. **Managers** includes any College associate that has supervisory responsibilities. Managers have the same responsibilities as Users and may in some cases may be assigned as Data Stewards or Access Administrators. In addition, they have responsibility for ensuring compliance with this policy for all Users they manage or supervise.

F. **Information Systems (IS) Department** is responsible for maintaining a secure computing environment for all systems and applications under its direct control that provides at a minimum to the extent technically feasible:

1. Secure user authentication protocols including:

    a. User account names and other identifiers.

    b. Secure methods of assigning passwords, or use of unique identifier technologies, multi-factor authentication, biometrics, or token devices.

    c. Control of passwords to ensure that such passwords are in a location and/or format that does not compromise the security of the data they protect.

    d. Restricting access to active Users and active User accounts only.

    e. Blocking access to User accounts after multiple unsuccessful attempts to gain access to a particular system.

2. Secure access control measures that:

    a. Restrict access to records and files containing Sensitive College Data to those who need such information to perform their job duties.

    b. Assign unique credentials to each person with privileged computer access to maintain the integrity of the security of the access controls.

3. Encryption of all transmitted records and files containing Sensitive College Data that will travel across public networks.

4. Encryption of all Sensitive College Data transmitted wirelessly.

5. Reasonable monitoring of systems for unauthorized use or access to Sensitive College Data.

6. Encryption of all Sensitive College Data stored on laptops or other portable devices.

7. For Internet connected systems that contain Sensitive College Data, up-to-date firewall protection and timely security patches, designed to maintain the security, integrity, and availability of Sensitive College Data.

8. Up-to-date versions of system software that must include malware protection and up-to-date patches and malware definitions, and is set to receive the most current security updates on a regular basis.

9. Education and training of employees on the proper use of the secure computing environment and the importance of data security.

10. Appropriately secure methods of remote and third party access to the College Network to authorized parties. (College Network means the system of computers, laptops, servers, storage devices, printers, and other related equipment owned by the College and used to process, transmit, receive, store, and otherwise manage College Data.)

11. Methods for maintaining the security of physical data housed offsite, including during transmission, storage, or destruction.

12. Methods for maintaining security of external cloud-based systems or platforms, including during transmission, storage, or destruction.

13. Methods for selecting and working with cloud-based platforms in terms of security, storage, and maintenance of all data types.

G. **Human Resources Department** is responsible for:

1. Maintaining a master list of all associate job titles, descriptions, and User access rights.

2. Maintaining a list of all current Data Stewards and Access Administrators.

3. Working with Data Stewards to develop access right roles based on job titles or descriptions.

4. Working with Access Administrators to manage data access rights.

5. Distributing this policy to all Associates and confirming their acceptance.

6. Developing data security training modules in cooperation with the Information Systems Department.

7. Delivering data security training and verifying completion by all associates.

CHAPTER 3 – DATA CLASSIFICATION AND CONTROL

A. Data Classification

1. **College Data** (or "College Information") means any data that is collected, maintained, or utilized by the College for the purpose of carrying out institutional business. College Data is divided into three classifications:

    a. Legally Protected Data;

    b. Non-Public Data; and

    c. Public Data.

2. **Legally Protected Data** means certain types of information that must be kept confidential and protected from unauthorized access or disclosure in accordance with federal and state laws and regulations, including, but not limited to, social security numbers; bank account numbers; driver's license numbers; student loan information; grades; transcripts; and health information. (See Appendix A.)

3. **Non-Public Data** means information that must also be kept confidential and protected from unauthorized access or disclosure but may not be legally protected. Non-Public Data includes, but is not limited to, competitively sensitive information (such as College proprietary, planning, strategy, operations, and financial information); information subject to a non-disclosure agreement; and personal directory information of associates. (See Appendix A.)

4. Note: Legally Protected Data and Non-Public Data may be collectively referred to as "**Sensitive College Data**."

5. **Public Data** includes any information that is easily accessible from public records, may be released without written consent, and/or is generally not considered harmful or an invasion of privacy if disclosed. Public Data includes, but is not limited to, student Directory Information as defined in the College's Student Records (FERPA) Policy and information accessible through the College's public website berkeleycollege.edu. (See Appendix A).

B. Data Control

1. All College Data shall have designated Data Stewards assigned by the Functional Vice President.

2. Data Stewards shall be responsible for protecting all Sensitive College Data within their control.

3. Data Stewards shall be responsible for assigning each category of their designated data as one of the following classifications above.

4. This policy provides the minimum requirements to protect Sensitive College Data. If the minimum requirements are not commensurate with risks posed to the data that a Data Stewards is responsible for, they shall develop and implement enhanced policies and security measures as necessary to safeguard the data for which they are responsible.

CHAPTER 4 – DATA ACCESS CONTROL

A. Berkeley College adheres to the "principle of least access." Users should be permitted access only to information they need to perform their job functions, and only for as long as reasonably necessary to accomplish that purpose. No User shall have access to Sensitive College Data unless there is a legitimate business purpose for such access.

B. Data Stewards are responsible for determining the appropriate level of User access rights to College Data.

C. No one shall be authorized to grant access rights to any College application or database without the formal approval of the appropriate Data Steward. Access right granting privileges for an individual may be revoked at any time at the discretion of the Data Steward.

D. Data Stewards must conduct an annual review of all Users within their department or functional area with permission to grant access rights to their data and verify that no one without proper authorization has been granted or retains those rights. Data Stewards must take immediate action through HR or IS to correct any inaccuracies or errors found

E. Each Data Steward is responsible for designating Access Administrators who are responsible for administering access to the data system(s) for which the Data Steward is responsible. Each data system must have at least two Access Administrators (one primary and one or more secondary).

F. An Access Administrator shall not grant a User new access rights, modify a User's existing access rights, or reduce a User's access rights unless explicitly approved by the appropriate Data Steward(s) and/or the Human Resources Department in accordance with this chapter.

G. Managers in line of authority are responsible for ensuring that associates they supervise have proper access rights in order to perform their job responsibilities. In the event that an associate requires new access rights, modification of existing access rights, or a reduction in access rights, the Manager must promptly submit a request for change to the appropriate Data Steward(s) using the Login Access Change form. Once approved by the Data Steward(s), the request for change shall be forwarded to the appropriate Access Administrator(s) to implement the change.

H. The Human Resources Department may assign basic access rights to new associates in lieu of Data Steward(s) where such access rights are included in approved job descriptions. When time is of the essence, the Human Resources Department may authorize Access Administrators to reduce or eliminate an associate's access rights. Human Resources is responsible for notifying the appropriate Data Steward upon submitting this type of request promptly.

I. The Human Resources Department shall maintain an up-to-date master list of Data Stewards and Access Administrators. Functional Vice Presidents, Managers, Data and/or an Access Administrators must promptly report the separation of an existing Data Steward and/or Access Administrator to the Human Resources Department.

J. The Human Resources Department shall maintain an up-to-date master list of access rights granted to each associate.

K. The Data Stewards must review the list of assigned Access Administrators and access rights lists annually, and provide updated information or actions as necessary.

L. The Information Systems Department is responsible for assigning and maintaining access to the College Network infrastructure and telecommunications systems.

M. The Data Stewards must ensure the enablement of appropriate activity tracking or auditing capabilities on each data system as determined by the Data Steward(s) in consultation with the Information Systems Department.

CHAPTER 5 – PASSWORD CONTROL

A. Strong passwords are required for any systems which provide access to Sensitive College Data.

B. Multi-factor authentication is to be enabled where systems support such authentication mechanisms.

C. Users must not share passwords with anyone, including Managers and members of the Information Systems Department.

D. Users must report any request for their passwords to their Manager or the Information Systems Department as appropriate.

E. If a User knows or has reason to believe any Berkeley College password (whether the User's password or another associate's password) has been disclosed or otherwise compromised, the password must be immediately changed or inactivated. The User must immediately report this to the Information Systems HelpDesk as a Data Security Incident.

F. If passwords are documented on paper, such paper must be stored in a secure locked location. Passwords that are stored electronically must be stored securely or encrypted.

G. Passwords must:

1. be changed every 90 days
2. have at least 8 characters
3. include both uppercase and lowercase letters
4. have at least 1 special character (not letter or digits)
5. have at least 1 letter
6. have at least 1 digit
7. not be the profile ID or name rearranged
8. contain elements from three of the four following types of characters: uppercase letters, lowercase letters, digits, punctuation marks or other symbols
9. not contain your username or any part of your full name
10. have at most 2 pairs of repeating characters
11. contain only characters available on a standard English (US) keyboard
12. not be an old password

H. Any system that provides access to Sensitive College Data must be configured to lock out a user after multiple unsuccessful password attempts, if this feature is available on such system.

I. Web browsers must not be set to remember or otherwise store passwords. This does not apply to single-sign on or multi-factor authentication tokens.

CHAPTER 6 – STORAGE OF SENSITIVE COLLEGE DATA

A. Sensitive College Data must be securely stored at all times to prevent access by unauthorized individuals.

B. Sensitive College Data in electronic format that is not stored on the College Network or another College-approved secure network must be encrypted.

C. Any Portable Digital Media or Mobile Device (as defined in Chapter 9) that contains Sensitive College Data must not be left unattended and must be securely stored in a locked drawer or cabinet when not in use.

D. Paper containing Sensitive College Data must never be left unattended and must be stored in a locked cabinet when not in use, in accordance with the Clean Desk Policy in Chapter 11.

E. Off-site storage and cloud vendors, including, but not limited to, Software as a Service (SaaS) platforms, Artificial Intelligence service providers, and other online service providers must meet security requirements that are commensurate with the risk posed to the data being processed, transmitted, received,stored or otherwise handled by the third party.

CHAPTER 7 – DISTRIBUTION AND TRANSMISSION OF SENSITIVE COLLEGE DATA

A. Sensitive College Data must not be distributed or made available to anyone who is not authorized to access the information. Sensitive College Data that is transmitted electronically, transported physically, or spoken in conversation must be appropriately protected from unauthorized interception.

B. Sensitive College Data in electronic format which is transmitted by any means other than the College Network, other approved secure network, off-site storage, or cloud must be encrypted in transit through appropriate techniques.

C. Sensitive College Data cannot be transmitted to, stored in, or otherwise handled by a non-approved network, off-site storage, or cloud environment, including, but not limited to, Software as a Service (SaaS) platforms, Artificial Intelligence service providers, and other online service providers.

D. Avoid distributing Sensitive College Data in paper form unless there is a valid business reason for doing so.

E. Sensitive College Data must be distributed using a trusted delivery method such as by hand or by College interoffice mail. Sensitive College Data which must be delivered by courier is to be sent certified mail-return receipt requested or by a recognized commercial courier (such as UPS or FedEx) which provides delivery and receipt tracking.

F. When Sensitive College Data is distributed from one person to another, the sender must confirm receipt with the intended recipient.

G. Whenever telephone or in-person conversations involve Sensitive College Data, the individuals authorized to know such information must be aware of their surroundings to prevent accidental disclosure of Sensitive College Data.

H. Sensitive College Data should not be stored "in the cloud" (such as Google Drive or iCloud, or other Software as a Service (SaaS) platforms) or submitted to or processed by an Artificial Intelligence service provider without authorization from the Chief Information Officer.

I. Sensitive College Data must not be shared with vendors or consultants until a non-disclosure agreement has been signed (and, where appropriate, a Network Access Agreement).

CHAPTER 8 - NETWORK AND CLOUD SECURITY

A. The Information Systems Department is responsible for:

1. Protecting the College Network from outside and inside threats such as intrusion, probing, viruses, spyware, malware, ransomware, denial-of-service attempts, and other security threats.

2. Evaluating the seriousness and immediacy of any threat to the College Network and taking action to mitigate that threat.

3. Maintaining standard procedures to protect Sensitive College Data commensurate with the risk posed to the Sensitive College Data.

B. Systems outside of the College Network that are not implemented, controlled, or maintained by the Information Systems department cannot be used to process or store Sensitive College Data unless authorized by the Information Systems department.

C. Users are responsible for complying with all rules, regulations, and policies established to protect the security, integrity, and availability of the College Network.

CHAPTER 9 – MOBILE DEVICE AND PORTABLE DIGITAL MEDIA SECURITY

Mobile Device means any computer, laptop, personal digital assistant, cell phone, smart phone, tablet, telephone, or other device which is designed to be portable and can store data or connect to a computer network or the Internet.

Portable Digital Media (or "PDM") means any digital media that is designed to be portable such as flash drives, CDs, DVDs, tapes, floppy disks, memory sticks, and portable hard drives.

Policy:

A. Mobile Devices and/or PDM which allow access to Sensitive College Data or to systems which contain Sensitive College Data must be password protected.

B. Once a User has logged into the Mobile Device or accessed the PDM, it must not be left unattended. When finished using the Mobile Device and/or PDM, a User must log out or lock it as to require a password and the device must remain in possession of the User until it can be securely stored.

C. Sensitive College Data must not be stored on a Mobile Device or PDM unless there is an approved legitimate academic, administrative, or other business reason for doing so.

D. Sensitive College Data must be securely erased from a Mobile Device or PDM immediately when it is no longer required.

E. When a Mobile Device or PDM is permanently transferred from one User to another, any Sensitive College Data on the device must be securely erased before transfer.

F. Any Mobile Device that is not owned, leased, or rented by the College but is personally owned and maintained by a User must be enrolled and registered in the Information Systems Department mobile device management program.

G. Any Mobile Device that has any Sensitive College Data stored on it must be encrypted using current cryptographically secure means. The Information Systems Department ensures that all College equipment has the correct patches and updates to ensure compliance with this proper encryption.

H. No personally owned Mobile Devices or other Internet connected devices are allowed to be connected to the College Network without approval from the Information Systems Department.

I. All Sensitive College Data stored on PDM must be password protected, encrypted, or otherwise securely protected from loss or unauthorized access.

J. The loss, theft, or inability to account for any Mobile Device and/or PDM containing Sensitive College Data must be reported promptly to the Help Desk as a Data Security Incident as described in Chapter 14.

CHAPTER 10 – REMOTE ACCESS

A. Users shall be granted remote access to the College Network only for legitimate academic, administrative, or business purpose(s).

B. The College Network may be remotely accessed only by using methods of connection approved by the Information Systems Department.

C. Users are responsible for safeguarding the remote access credentials granted to them in accordance with this policy. These credentials may consist of username and password combinations, digital certificates, or other software and/or hardware.

D. All computers or other devices to be used for remote access to the College Network must meet the standards established by the Information Systems Department and must be available for inspection upon request by a representative of the Information Systems Department in order to verify compliance with this policy.

E. Accessing Sensitive College Data remotely from a public device is not permitted.

F. When a User utilizes a personally owned mobile device, tablet, or computer to access Sensitive College Data, the User must ensure that the machine is up-to-date on all security patches, and has current and updated anti-virus and anti-malware protection.

G. The loss or theft of any personally owned Mobile Device or PDM containing Sensitive College Data must be reported immediately to the Help Desk as a Data Security Incident.

CHAPTER 11 – PHYSICAL SECURITY

A. **Physical Entry Controls:** Areas containing Sensitive College Data in any form or access to any component of the College Network must be protected by appropriate physical entry controls to ensure that only authorized personnel are allowed access. Visitors to secured areas must be supervised by authorized personnel.

B. **Server Rooms**: College Network server rooms must be locked at all times. Public Safety and Campus Operations are responsible for monitoring and logging access to these locations. Visitors to server rooms must be accompanied by authorized staff or other designee of the Information Systems Department.

C. **Clean Office and Desk Area Policy:** Individual offices and work areas utilized by Users with access to Sensitive College Data must be kept secure.

   1. Doors are to be locked when Users are not present.

   2. Sensitive College Data must not be viewable by passersby or unauthorized individuals (including guests and unauthorized Users).

   3. Computer monitors must be carefully positioned so that viewing is restricted to the authorized User.

   4. When leaving a computer unattended in a location where it might be accessed by unauthorized individuals, the User must either log out of all networks and applications or utilize a password-protected screensaver.

   5. Sensitive College Data in physical form must be covered or put away when unauthorized individuals are present.

   6. Any PDM containing Sensitive College Data or other Sensitive College Data in physical form must be kept in a locked drawer, cabinet, or storage area when (1) not in use; (2) when left unattended, including at the end of the work day; or (3) any time the User is out of the office.

   7. Users should lock their office door at the end of the work day or any time the user is gone for an extended period of time. Users who do not have an office with a door that locks must keep Sensitive College Data in physical form in a locked drawer.

J. **Equipment Security:** Equipment components of the College Network, including individual computers, are to be secured using a locking mechanism where feasible.

K. **Secure Disposal of Equipment**: All equipment and component devices containing Berkeley College Data must be checked to ensure that any College Data is securely erased prior to disposal. Equipment will be securely erased by the Information Systems Department.

CHAPTER 12 – THIRD PARTY ACCESS

A. Any third party (such as a consultant) accessing Sensitive College Data remotely must enter into a Non-Disclosure Agreement, Network Access Agreement, and agree to comply with this Policy and all other applicable College policies.

B. Third party access to the College Network may be made for legitimate academic, administrative, or business purposes only.

C. Requests to allow a third party access to the College Network must be authorized by the Information Systems Department and the relevant Data Steward(s) prior to access being granted.

D. The requester is responsible for assuring that the third party signs the required Non-Disclosure Agreement, Network Access Agreement, and agrees in writing to comply with all applicable College policies..

E. In order to ensure individual accountability on the College Network, each third party granted access must be given a unique user identification and password. The third party will at all times be held responsible for any activities which occur on the College Network using this unique user identification.

  1. In certain cases, a third party may be given access to a generic account (such as an email account) in order to perform their contractual obligations. In such circumstances, the third party's activity must be closely monitored by the requester and/or another member of the department working with the third party.

CHAPTER 13 – DISPOSAL OF SENSITIVE COLLEGE DATA

A. **Disposal of Sensitive College Data**: When there is no legal, business or other legitimate reason to store Sensitive College Data, such Sensitive College Data must be disposed of as follows:

1. Shred any paper containing Sensitive College Data.

2. Securely erase or physically destroy, as required, any media containing other Sensitive College Data in electronic format as directed by the Information Systems Department.

3. Information Systems will employ a third-party vendor to store and certify thedestruction of all physical data medium as required, in accordance with the College data retention policies.

L. **Disposal of Public Data:** When there is no legal, business, or other legitimate reason to store Public Data, such data is to be disposed of as follows:

1. Shred any paper containing Public Data wherever possible; if shredding is not required, it must be recycled.

2. Securely erase or physically destroy, as required, any media containing Public Data in electronic format as directed by the Information Systems Department.

M. **Transfer of Computers and Other Devices:** The Information Systems Department will securely erase all College Data stored on a computer, mobile device, or other equipment with the capacity to store data when transferring the device from one User to another.

N. **Responsibilities:**

1. Data Stewards shall be responsible for establishing procedures for the disposal of Sensitive College Data.

2. Campus Operating Officers shall be responsible for maintaining shredding and recycling facilities at their campus locations.

3. The Information Systems Department shall be responsible for establishing procedures for securely erasing or destroying electronic College Data.

CHAPTER 14 – DATA SECURITY INCIDENTS

Data Security Incident means any incident where any Sensitive College Data is suspected to have been breached or compromised in any way. This includes examples such as accidental disclosure, loss of equipment containing Sensitive College Data, or malicious activity.

A. All observed or suspected Data Security Incidents must be promptly reported to theInformation Systems Helpdesk as a Data Security Incident. Users must not attempt to investigate or resolve an incident on their own.
B. The Helpdesk will notify the Chief Information Security Officer who will direct an investigation of the incident and take any appropriate immediate actions to mitigate and/or remediate (including, but not limited to, changing or restricting account access; password resets; and remote erasure).
C. If the Chief Information Security Officer determines there is a reasonable likelihood that Sensitive College Data may have been disclosed to unauthorized individual(s), the Core Incident Response Team will be notified.
D. The Core Incident Response Team will consist of the Chief Information Security Officer, Chief Information Officer, and a representative from the Office of General Counsel and Communications and External Relations Department. The Team will consult with Human Resources and the Office of the Provost, as appropriate, contingent upon the nature of the incident.
E. The Core Incident Response Team will review the conclusions of the Investigative Team andwill present a recommended response to the President. The Emergency Management Master Plan will be invoked if appropriate.

CHAPTER 15 – LOSS OR THEFT OF COLLEGE EQUIPMENT

A. If College computer equipment is lost or stolen, the equipment holder or associate discovering the loss must notify the Information Systems HelpDesk and report the loss or theft as a Data Security Incident.

B. An explanation given by the equipment holder describing the circumstances surrounding the loss or theft must accompany all reports. This information will be kept on file by the Information Systems Department as part of the Data Security Incident report.

C. Replacement equipment, if any, will be determined by the Information Systems Department in consultation with the associate’s manager.

CHAPTER 16 – COLLEGE DATA AWARENESS

A. All associates are responsible for reviewing this Data Security Policy and affirmatively agreeing to comply with it. The Human Resources Department shall be responsible for distributing this Data Security Policy and tracking acceptance by associates.

B. During orientation, all new full and part-time associates, temporary workers, and volunteers must be instructed on the importance of information security and their roles in protecting Sensitive College Data.

C. Classes (online or in-person) shall be held annually to continue to educate associates about this policy and the importance of protecting College Data. The Human Resources Department shall track successful completion of these classes.

D. Managers in line of authority shall ensure that associates under their supervision are aware of this Data Security Policy and other relevant information security policies, procedures, and guidelines, and have access to current versions. If modifications to policies are distributed, managers must inform their respective communities as soon as possible.

E. Managers in line of authority shall hold awareness and education sessions on an annual basis to review any information security practices and policies that supplement this policy with associates under their supervision.

F. Third parties authorized to access Sensitive College Data must be informed of their responsibilities under this Data Security Policy. Authorized third parties shall have College information security awareness and educational materials made available for use.

CHAPTER 17 – PERIODIC POLICY REVIEW

A. A Data Security Policy Review Committee made up appropriate Information Systems managers and other representatives of College departments shall meet annually to review this policy and recommend any changes.

B. The chairperson of the Data Security Policy Review Committee shall be the Chief Information Officer.

C. The recommendations of the Data Security Policy Review Committee shall be submitted to the President for approval.

APPENDIX

Categories of College Data

A. Sensitive Data

1. Legally Protected Data

Below are examples of information that must be kept strictly confidential and protected from unauthorized access and disclosure, in accordance with federal and state laws and regulations.

Identity Data

Social security number
Bank/financial account number
Citizenship/nationality/visa status
Credit/debit card number
Driver's license number
Medical records
Passport number
Passwords
Age/Date of birth
Place of birth
Mother's maiden name
Income tax records

Student and Alumni Data*

Academic status
Admissions records
Class level
Counseling records
Course schedule
Course evaluations
Disability records
Disciplinary records
Ethnicity, race, and national origin
Fees (assessed or paid)
Financial aid records
Financial statements (student or parent/guardian)
Gender
Grades (including GPA)

Healthcare providers
Instructors
Letters of recommendation
Loan collection records
Parent/Guardian name and address
Payroll records (Federal Work Study)
Residency status
Selective Service/Veteran's Administration Status
Special programs
Student Accounts records
Tests, exams, and papers
Transcripts

***NOTE:** The College may release student information in limited circumstances, as outlined in the College's Student Records (FERPA) Policy.

2. Non-Public Data

Below are examples of information that must be kept confidential and protected from unauthorized access or disclosure.

Associate Data

Biographical information
Compensation
Disciplinary records
Employee benefits elections
Employee ID number
Employment applications
Faculty transcripts
Faculty evaluations
Family member/beneficiary information
Grievances
Home address
Home telephone number
Performance evaluations
Personal email address
Student instructional reports (SIRS)
Whistleblower records
Worker's compensation claims

Business and Financial Records

Audit/investigative work papers and reports

Bank/financial account records
Data subject to confidentiality/non-disclosure agreements
Financial statements
Information related to business operations and strategies
Internal policies and procedures
Injury and damage claims
Litigation records
Marketing plans
Proprietary vendor information
Tax returns
Trade secrets

Facilities
Architectural records and floor plans
Building systems equipment locations
Hazardous materials locations and details
Utility valve locations

B. Public Data

Below are examples of Public Data that is easily accessible from public records, may be released without written consent, and/or is generally not considered harmful or an invasion of privacy if disclosed.

Student Data (Directory Information)*

Full name
Address
Phone number
Email address
Student ID number
Date and place of birth
Major field(s) of study
Participation in officially recognized activities and sports
Dates of attendance
Degrees
Honors and awards received
Most recent previous school attended
Likeness (photograph, video, or other form)

***NOTE:** The College is permitted to release Directory Information in accordance with the Student Records (FERPA) Policy. In certain cases, Directory Information must be treated as **Legally Protected Data** for students who have submitted a Directory

Information Opt-Out e-form the Registrar's Office. The College is prohibited from sharing Directory Information about students who have submitted this form (without their written consent).

Associate Data

Full name
College title
College department
College office address
College phone number
College email address

Other Data

All publicly available information on berkeleycollege.edu
All publicly available information on Berkeley College social media
College press releases
College newsletters
External job postings and job descriptions

C. Financial Aid Data:

ISIR data and FTI (Federal Tax information) from the IRS must be treated differently, FTI is considered Controlled Unclassified Information (CUI)

ISIR data, which includes the Student Aid Index (SAI) may only be shared with staff members at the college, other than Financial Aid Administrators (FAA)s, they have been designated to be part of the financial aid process. These people reside in:

Admissions
Student Accounts
Institutional Effectiveness

FTI – may not be shared with anyone, other than FAAs, with the exception of:

Students
Institutional Effectiveness, as needed, for Federal and State Reporting
College contractors that perform financial aid award functions
Scholarship organization, but only with expressed written approval of the student

FTI Data elements include:

Tax year
Tax filing status
Adjust Gross Income (AGI)
Number of exemptions and dependents

Income earned from work
Taxes paid
Educational credits
Untaxed IRS distributions
IRA deductible and payments
Tax exempt interest
Untaxed pension amounts
Schedule C net profit/loss
Indicators for Schedules
IRS Response Code

- Shared ISIR and FTI data must be accomplished in a secure manner at all times
- FTI must be appropriately marked, and handled
- FTI must retain the CUI labeling where data is stored
- Labels must be present when FTI is inspected or used
- The use of FTI, for the purpose of research, is strictly prohibited

Other FTI Sharing:

- We may share all contributor's FTI with the student.
- Other contributors (not the student) may only have access to their own FTI.
- We may share FTI, with scholarship organizations, only after the student has sign a consent to do so for the specific entity.